Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS)

Conditions et procédures d'évaluation de sécurité

Version 1.2
Octobre 2008

Modifications apportées au document

Date	Version	Description
1er Octobre 2008	*1.2*	*Aligner le contenu avec la nouvelle procédure PCI DSS v1.2 et implémenter les changements mineurs notés depuis la v1.1 d'origine.*

Copyright 2008 PCI Security Standards Council LLC

Table des matières

Modifications apportées au document ..... **i**

Introduction ..... **iv**

Objectif de ce document iv
Relation entre PCI DSS et PA-DSS iv
Portée de la norme PA-DSS v
Conditions d'application de la norme PA-DSS aux terminaux matériels vi
Rôles et responsabilités vi
Guide de mise en œuvre de la norme PA-DSS ix
Exigences relatives aux PA-QSA x
Laboratoire de test x

Informations relatives aux conditions d'application des normes PCI DSS ..... **xi**

Instructions et contenu du Rapport sur la conformité ..... **xii**

Étapes de mise en conformité avec la norme PA-DSS ..... **xiv**

Guide du programme de la norme PA-DSS ..... **xiv**

Conditions et procédures d'évaluation de sécurité de la norme PA-DSS **1**

1. Ne pas conserver la totalité des données de bande magnétique, de code ou de valeur de validation de carte (CAV2, CID, CVC2, CVV2), ou de bloc PIN 1
2. Protéger les données de titulaire de carte stockées 5
3. Fournir des fonctions d'authentification sécurisées 8
4. Enregistrer l'activité des applications de paiement 10
5. Développer des applications de paiement sécurisées 11
6. Protéger les transmissions sans fil 16
7. Tester les applications de paiement pour gérer les vulnérabilités 17
8. Permettre la mise en œuvre de réseaux sécurisés 18
9. Les données de titulaire de carte ne doivent jamais être stockées sur un serveur connecté à Internet. 18
10. Permettre des mises à jour logicielles à distance sécurisées 19
11. Permettre un accès à distance sécurisé à l'application de paiement 19
12. Crypter le trafic sensible transitant par les réseaux publics 22
13. Crypter tous les accès administratifs non-console 23
14. Gérer la documentation fournissant des instructions et les programmes de formation pour les clients, les revendeurs et les intégrateurs. 23

Copyright 2008 PCI Security Standards Council LLC

Annexe A : Résumé du contenu du *Guide de mise en œuvre de la norme PA-DSS* 25
Annexe B : Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS 31
Annexe C : Attestation de conformité 36

Copyright 2008 PCI Security Standards Council LLC

Introduction

Objectif de ce document

Ce document est destiné aux PA-QSA (Payment Application-Qualified Security Assessors, évaluateurs de sécurité qualifiés des applications de paiement) responsables de l'examen des applications de paiement, afin que les fournisseurs de logiciels puissent valider la conformité d'une application de paiement avec la norme PA-DSS (Payment Application Data Security Standard, ou norme de sécurité des données des applications de paiement PCI DSS). Ce document doit également être utilisé par les évaluateurs PA-QSA comme modèle pour l'élaboration du Rapport sur la conformité.

Relation entre PCI DSS et PA-DSS

Les exigences de la PA-DSS sont issues des *conditions et procédures d'évaluation de sécurité des normes PCI DSS*. Ce document, disponible sur le site www.pcisecuritystandards.org, décrit ce qui doit être conforme aux normes PCI DSS (et, par conséquent, ce que doit prendre en charge une application de paiement pour assurer la conformité du client avec les PCI DSS).

Il se peut que la conformité conventionnelle avec les normes PCI DSS ne s'applique pas directement aux fournisseurs d'applications de paiement car la plupart des fournisseurs ne stockent, ne traitent et ne transmettent pas de données de titulaire de carte. Cependant, étant donné que ces applications de paiement sont utilisées par les clients pour stocker, traiter et transmettre des données de titulaire de carte, et que les clients sont dans l'obligation de respecter les normes PCI DSS, les applications de paiement doivent permettre au client (et non l'empêcher) de se conformer aux normes PCI DSS. Voici quelques exemples sur la façon dont les applications de paiement peuvent faire obstacle à la conformité :

1. Stockage des données de bande magnétique sur le réseau du client après autorisation.
2. Applications nécessitant que les clients désactivent d'autres fonctions requises par les normes PCI DSS, telles que des programmes antivirus ou des pare-feu, afin que l'application de paiement fonctionne correctement.
3. Utilisation par le fournisseur de méthodes non sécurisées pour se connecter à l'application afin d'apporter une assistance au client.

Les applications de paiement sécurisées, lorsqu'elles sont mises en œuvre dans un environnement conforme PCI DSS, réduisent autant que possible le risque de voir les failles de sécurité compromettre les données de bande magnétique, les codes et valeurs de validation de carte (CAV2, CID, CVC2, CVV2), les codes et les blocs PIN, ainsi que la fraude résultant de ces failles.

Copyright 2008 PCI Security Standards Council LLC

Portée de la norme PA-DSS

La norme PA-DSS s'applique aux fournisseurs de logiciels et autres fournisseurs qui développent des applications de paiement stockant, traitant ou transmettant des données de titulaire de carte dans le cadre d'une autorisation ou d'un règlement, lorsque ces applications de paiement sont vendues, distribuées ou cédées sous licence à des parties tierces.

Le guide suivant peut être utilisé pour déterminer si la norme PA-DSS s'applique à une application de paiement donnée :

Remarque :

Les produits validés d'application de paiement ne peuvent en aucun cas être des versions bêta.

- La norme PA-DSS s'applique aux applications de paiement généralement vendues « prêtes à l'emploi » sans modification apportée par les fournisseurs de logiciels.
- La norme PA-DSS concerne les applications de paiement fournies dans des modules, habituellement composés d'un module de base et d'autres modules spécifiques aux types de clients ou fonctions, ou personnalisés à la demande du client. Il se peut que la norme PA-DSS s'applique uniquement au module de base si ce module est le seul exécutant les fonctions de paiement (après confirmation par un PA-QSA). Si d'autres modules réalisent des fonctions de paiement, la norme PA-DSS s'applique également à ces modules. Notez que, pour les fournisseurs de logiciels, l'isolement des fonctions de paiement en un seul ou quelques modules de base (en réservant les autres modules pour les fonctions autres que le paiement) constitue une « meilleure pratique ». Cette meilleure pratique (bien qu'elle ne constitue pas une exigence) peut limiter le nombre de modules soumis à la norme PA-DSS.
- La norme PA-DSS NE s'applique PAS à une application de paiement développée pour un seul client et vendue à celui-ci, puisque cette application sera couverte dans le cadre de la vérification de conformité PCI DSS standard du client. Remarque : une telle application (que l'on peut qualifier d'application « sur mesure ») est vendue à un seul client (en général un commerçant ou un prestataire de services important) et elle est conçue et développée selon les spécifications du client.
- PA-DSS NE s'applique PAS aux applications de paiement développées par des commerçants et des prestataires de services si elles sont utilisées en interne uniquement (et non vendues à une partie tierce), puisque de telles applications de paiement doivent être couvertes dans le cadre de la conformité normale du prestataire de services aux PCI DSS.

Par exemple, concernant les deux derniers points ci-dessus, le fait que l'application de paiement développée en interne ou sur mesure stocke des données d'authentification sensibles interdites ou autorise des mots de passe complexes doit être couvert dans le cadre de la conformité normale du commerçant ou du prestataire de services aux normes PCI DSS et ne requiert pas d'évaluation PA-DSS distincte.

La liste non exhaustive suivante fournit des exemples d'applications AUTRES que des applications de paiement pour les besoins de la PA-DSS (et qui, par conséquent, n'ont pas besoin d'être soumis aux vérifications PA-DSS) :

Remarque :

Le PCI SSC répertorie UNIQUEMENT les applications de paiement.

- les systèmes d'exploitation sur lesquels une application de paiement est installée (par exemple, Windows, Unix) ;
- les systèmes de base de données stockant des données de titulaire de carte (par exemple, Oracle) ;
- les systèmes de back office stockant les données de titulaire de carte (par exemple, pour les besoins de reporting ou du service client).

Copyright 2008 PCI Security Standards Council LLC

La portée de la vérification PA-DSS doit comprendre ce qui suit :

- Couverture de toutes les fonctions d'application de paiement, y compris mais sans s'y limiter 1) les fonctions de paiement complètes (autorisation et règlement), 2) les entrées et les sorties, 3) les conditions d'erreur, 4) les interfaces et les connexions à d'autres fichiers, systèmes et/ou à des applications de paiement ou à des composants d'application, 5) tous les flux de données de titulaire de carte, 6) les dispositifs de cryptage et 7) les dispositifs d'authentification.
- Assistance que le fournisseur de l'application de paiement est tenu de proposer aux clients et aux revendeurs/intégrateurs (voir le *Guide de mise en œuvre de la norme PA-DSS* ci-après) pour s'assurer que 1) le client sait comment mettre en œuvre l'application de paiement conformément aux normes PCI DSS et que 2) le client est clairement informé que certains paramètres des applications et environnements de paiement peuvent empêcher la conformité avec les normes PCI DSS. Notez que le fournisseur de l'application de paiement peut être tenu de fournir de telles directives, y compris lorsque le paramètre concerné 1) ne peut pas être contrôlé par le fournisseur une fois l'application installée par le client ou 2) dépend de la responsabilité du client, et non du fournisseur de l'application de paiement.
- Couverture de toutes les plates-formes sélectionnées pour la version vérifiée de l'application de paiement (les plates-formes incluses doivent être indiquées).
- Couverture des outils utilisés par ou au sein d'une application de paiement pour accéder et/ou consulter des données de titulaire de carte (outils de reporting, de journalisation, etc.).

Conditions d'application de la norme PA-DSS aux terminaux matériels

Les terminaux matériels dotés d'applications de paiement résidentes (également appelés terminaux de point de vente légers ou autonomes) n'ont pas besoin d'être soumis à une vérification PA-DSS *si* ***toutes*** *les conditions suivantes sont remplies* :

- Le terminal n'est connecté à aucun système ou réseau du commerçant.
- Le terminal se connecte uniquement à l'acquéreur ou au processeur.
- Le fournisseur de l'application de paiement propose 1) des mises à jour, 2) un dépannage, 3) un accès et 4) une maintenance à distance et sécurisés.
- Les éléments suivants ne sont jamais stockés après autorisation : la totalité du contenu de toute piste d'une bande magnétique (située au verso de la carte, de la puce ou autre), le code ou valeur de validation de carte (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement), le code PIN ou le bloc PIN crypté.

Rôles et responsabilités

Il existe plusieurs parties prenantes au sein de la communauté des applications de paiement. Certaines de ces parties prenantes participent plus directement que d'autres au processus d'évaluation PA-DSS (fournisseurs, QSA et PCI SCC). D'autres, non directement impliquées dans le processus d'évaluation, doivent avoir connaissance du processus global afin de faciliter les décisions professionnelles s'y rapportant.

Les sections suivantes définissent les rôles et responsabilités des parties prenantes dans la communauté des applications de paiement. Les responsabilités associées au processus d'évaluation sont mentionnées pour les parties prenantes impliquées.

Copyright 2008 PCI Security Standards Council LLC

Marques de cartes de paiement

American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. sont les marques de cartes de paiement qui ont fondé le PCI SSC. Elles sont responsables du développement et de l'application de tous les programmes relatifs à la conformité avec la norme PA-DSS, y compris des éléments suivants (liste non exhaustive) :

- toute exigence, mandat ou date pour l'utilisation des applications de paiement conformes à la norme PA-DSS ;
- toute amende ou pénalité relative à l'utilisation d'applications de paiement non conformes.

Les marques de cartes de paiement peuvent définir des programmes de conformité, des mandats, des dates, etc., basés sur la norme PA-DSS et les applications de paiement conformes listées par le PCI SSC. Via ces programmes de conformité, les marques de cartes de paiement font la promotion des applications de paiement conformes listées.

Payment Card Industry Security Standards Council (PCI SSC)

Le PCI SSC (Payment Card Industry Security Standards Council, conseil sur les normes de sécurité du secteur des cartes de paiement) est l'organisme de normalisation qui gère les normes du secteur des cartes de paiement, dont les normes PCI DSS et PA-DSS. En ce qui concerne la norme PA-DSS, le PCI SSC :

- constitue un site de stockage centralisé pour les rapports sur la conformité PA-DSS ;
- réalise des analyses d'assurance qualité sur les rapports sur la conformité PA-DSS, afin de vérifier la cohérence et la qualité des rapports ;
- dresse sur le site Web la liste des applications de paiement conformes à la norme PA-DSS ;
- assure la qualification et la formation des PA-QSA pour réaliser des vérifications PA-DSS ;
- gère et met à jour la norme PA-DSS et la documentation connexe selon un processus de gestion du cycle de vie des normes.

Remarque : Le PCI SSC ne valide pas la conformité des rapports. Le rôle des PA-QSA est de documenter la conformité de l'application de paiement à la norme PA-DSS, à la date de l'évaluation. Le PCI SSC réalise en outre une analyse d'assurance qualité afin de garantir une documentation précise et complète par les PA-QSA des évaluations PA-DSS.

Fournisseurs de logiciels

Les fournisseurs de logiciels (ci-après dénommés « les fournisseurs ») développent les applications de paiement qui stockent, traitent ou transmettent des données de titulaire de carte dans le cadre d'une autorisation ou d'un règlement, puis vendent, distribuent ou cèdent sous licence ces applications de paiement à des parties tierces (clients ou revendeurs/intégrateurs). Responsabilités des fournisseurs :

- Création d'applications de paiement conformes à la norme PA-DSS qui permettent, et n'empêchent pas, la conformité avec les normes PCI DSS de leurs clients. (L'application ne peut pas imposer un paramètre de mise en œuvre ou de configuration enfreignant une exigence des normes PCI DSS.)
- Respect des exigences des normes PCI DSS chaque fois que le fournisseur stocke, traite ou transmet des données de titulaire de carte (par exemple, lors du dépannage du client).
- Création d'un *Guide de mise en œuvre de la norme PA-DSS*, spécifique à chaque application de paiement, conformément aux exigences de ce document.

Copyright 2008 PCI Security Standards Council LLC

- Formation des clients, des revendeurs et des intégrateurs pour l'installation et la configuration des applications de paiement conformément aux normes PCI DSS.
- Assurance que les applications de paiement respectent les normes PA-DSS en passant avec succès une vérification PA-DSS comme spécifié dans ce document.

PA-QSA

Les PA-QSA sont des QSA (Qualified Security Assessors, évaluateurs de sécurité qualifiés) qualifiés et formés par le PCI SSC pour effectuer des vérifications PA-DSS. *Remarque : Tous les QSA ne sont pas des PA-QSA ; un QSA doit répondre à des exigences de qualification supplémentaires pour accéder au statut de PA-QSA.*

Responsabilités des PA-QSA :

- réaliser des évaluations des applications de paiement conformément aux procédures d'évaluation de sécurité et aux exigences de conformité des PA-QSA ;
- formuler un avis sur la conformité de l'application de paiement aux exigences de la norme PA-DSS ;
- fournir dans le rapport sur la conformité la documentation adéquate permettant de prouver la conformité de l'application de paiement à la norme PA-DSS ;
- transmettre le rapport sur la conformité au PCI SSC, accompagné de l'attestation de conformité (signée par le PA-QSA et par le fournisseur) ;
- gérer un processus interne d'assurance qualité appliqué à leurs tâches de PA-QSA.

Il appartient aux PA-QSA de spécifier si oui ou non l'application de paiement est conforme. Le PCI SSC ne valide pas les rapports sur la conformité au niveau de la conformité technique, mais réalise sur ceux-ci des analyses d'assurance qualité, afin de garantir que la preuve de la conformité soit correctement documentée dans les rapports.

Revendeurs et intégrateurs

Les revendeurs et les intégrateurs sont les entités qui vendent, installent et/ou interviennent sur les applications de paiement au nom de fournisseurs de logiciels ou autres. Responsabilités des revendeurs et des intégrateurs :

- mettre en œuvre d'une application de paiement selon la norme PA-DSS dans un environnement conforme aux normes PCI DSS (ou indiquer au commerçant d'agir ainsi) ;
- configurer l'application de paiement (lorsque des options de configuration sont fournies) selon le *Guide de mise en œuvre de la norme PA-DSS* remis par le fournisseur ;
- configurer l'application de paiement (ou indiquer au commerçant d'agir ainsi) conformément aux normes PCI DSS ;
- intervenir sur les applications de paiement (par exemple, dépannage, mise à disposition de mises à jour à distance et support distant) conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux normes PCI DSS.

Les revendeurs et les intégrateurs ne soumettent pas les applications de paiement à des évaluations. Seul le fournisseur peut soumettre des produits à évaluation.

Copyright 2008 PCI Security Standards Council LLC

Clients

Les clients sont les commerçants, les fournisseurs de services et autres qui achètent ou reçoivent une application de paiement pour stocker, traiter ou transmettre des données de titulaire de carte dans le cadre de l'autorisation ou du règlement des transactions de paiement. Les clients voulant utiliser des applications conformes à la norme PA-DSS sont chargés de :

- mettre en œuvre d'une application de paiement selon la norme PA-DSS dans un environnement conforme aux normes PCI DSS ;
- configurer l'application de paiement (lorsque des options de configuration sont fournies) selon le *Guide de mise en œuvre de la norme PA-DSS* remis par le fournisseur *;*
- configurer l'application de paiement conformément aux normes PCI DSS ;
- maintenir le statut de conformité aux normes PCI DSS pour la configuration de l'environnement et de l'application de paiement.

Remarque :

Une application de paiement conforme à la norme PA-DSS seule ne garantit pas la conformité avec les normes PCI DSS.

Guide de mise en œuvre de la norme PA-DSS

Les applications de paiement validées doivent pouvoir être mises en œuvre en conformité avec les normes PCI DSS. Les fournisseurs de logiciels sont dans l'obligation de fournir un *Guide de mise en œuvre de la norme PA-DSS* pour informer leurs clients et les revendeurs/intégrateurs sur la mise en œuvre sécurisée des produits, pour documenter les spécifications de la configuration sécurisée mentionnées tout au long de ce document et pour définir clairement les responsabilités des fournisseurs, des revendeurs/intégrateurs ainsi que des clients afin de satisfaire aux exigences des normes PCI DSS. Ce guide doit détailler la façon dont le client et/ou le revendeur/l'intégrateur doit activer les réglages de sécurité au sein du réseau du client. Par exemple, le *Guide de mise en œuvre de la norme PA-DSS* doit traiter des responsabilités et des fonctions de base de la sécurité par mot de passe des normes PCI DSS, même si cela n'est pas contrôlé par l'application de paiement, de façon à ce que le client ou le revendeur/l'intégrateur comprenne comment mettre en œuvre des mots de passe sécurisés afin d'assurer la conformité avec les normes PCI DSS.

Les applications de paiement, lorsqu'elles sont mises en œuvre conformément au *Guide de mise en œuvre de la norme PA-DSS* dans un environnement respectant les normes PCI DSS, doivent permettre et soutenir la conformité des clients avec les normes PCI DSS.

Reportez-vous à l'annexe A : Résumé du contenu du *Guide de mise en œuvre de la norme PA-DSS* pour comparer les responsabilités de la mise en œuvre des contrôles spécifiés dans ce *guide*.

Copyright 2008 PCI Security Standards Council LLC

Exigences relatives aux PA-QSA

- Seuls les PA-QSA (Payment Application Qualified Security Assessors, évaluateurs de sécurité qualifiés des applications de paiement) employés par les sociétés QSA (Qualified Security Assessor, évaluateur de sécurité qualifié) sont autorisés à réaliser des vérifications PA-DSS. Veuillez vous reporter à la liste des QSA à l'adresse www.pcisecuritystandards.org afin de connaître les sociétés qualifiées pour mener ces vérifications.
- Ces sociétés doivent utiliser les procédures de test documentées dans ce document sur la norme PA-DSS.

Laboratoire de test

- Le PA-QSA doit avoir accès au laboratoire où le processus de validation est censé intervenir. Ce laboratoire doit permettre de simuler une utilisation de l'application de paiement dans des conditions réelles.
- Veuillez vous reporter à l'*annexe B* : *Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS* de ce document pour connaître le détail des exigences applicables au laboratoire et aux processus de laboratoire afférents.
- Le PA-QSA doit renseigner l'annexe B et la renvoyer. Il doit la compléter pour le laboratoire spécifique qui sera utilisé pour l'application de paiement soumise à vérification. Cette annexe fait partie du rapport PA-DSS complété.

Copyright 2008 PCI Security Standards Council LLC

Informations relatives aux conditions d'application des normes PCI DSS

(Extrait de PCI DSS v1.2)

Le tableau ci-dessous issu des normes *PCI DSS* présente un certain nombre d'éléments communément utilisés des données de titulaire de carte et d'authentification sensibles, indique si le **stockage** de chaque élément de données est autorisé ou interdit, et précise si chaque élément de données doit être **protégé**. Ce tableau n'est pas exhaustif, mais il est présenté de manière à illustrer les divers types d'exigences qui s'appliquent à chaque élément de données.

Le PAN (Primary Account Number, numéro de compte principal) est le facteur de définition des conditions d'application des exigences PCI DSS et de la norme PA-DSS. Si le PAN n'est pas stocké, traité ou transmis, les normes PCI DSS et PA-DSS ne s'appliquent pas.

	Élément de données	Stockage autorisé	Protection requise	Exig. PCI DSS 3, 4
Données de titulaire de carte de crédit	PAN	Oui	Oui	Oui
	Nom du titulaire de la carte de crédit [1]	Oui	Oui [1]	Non
	Code service [1]	Oui	Oui [1]	Non
	Date d'expiration [1]	Oui	Oui [1]	Non
Données d'authentification sensibles [2]	Données de bande magnétique complètes [3]	Non	s.o.	s.o.
	CAV2/CID/CVC2/CVV2	Non	s.o.	s.o.
	Bloc/Code PIN	Non	s.o.	s.o.

[1] *Ces éléments de données doivent être protégés s'ils sont stockés conjointement avec le PAN. Cette protection doit être conforme aux exigences PCI DSS en liaison avec la protection générale de l'environnement des titulaires de carte. En outre, d'autres lois (par exemple, relatives à la protection des données personnelles des consommateurs, à la confidentialité, à l'usurpation d'identité ou à la sécurité des données) peuvent imposer une protection spécifique de ces données, ou une divulgation adéquate des pratiques de la société dès lors que des données à caractère personnel sont collectées dans le cadre de l'activité. Toutefois, les normes PCI DSS ne s'appliquent pas si des PAN ne sont pas stockés, traités ou transmis.*

[2] *Ne stocker aucune donnée d'authentification sensible après autorisation (même cryptée).*

[3] *Données de piste complètes extraites de la bande magnétique, de l'image de la bande magnétique sur la puce, ou d'un autre support.*

Copyright 2008 PCI Security Standards Council LLC

Instructions et contenu du Rapport sur la conformité

Ce document doit être utilisé par les évaluateurs PA-QSA comme modèle pour l'élaboration du Rapport sur la conformité. Tous les évaluateurs PA-QSA doivent suivre les instructions de ce document en ce qui concerne le contenu et la mise en forme lorsqu'ils complètent le Rapport sur la conformité.

Le Rapport sur la conformité doit comprendre les informations suivantes en préface des conditions et procédures d'évaluation de sécurité détaillées :

1. **Description de la portée de la vérification**
   - Description de la portée des éléments à couvrir lors de la vérification, en fonction de la section sur la portée de la norme PA-DSS ci-dessus
   - Calendrier de conformité
   - Version PA-DSS utilisée lors de l'évaluation
   - Liste de la documentation vérifiée
2. **Résumé**

   Inclure les éléments suivants :
   - le nom du produit ;
   - la version du produit et les plates-formes associées couvertes ;
   - la liste des revendeurs et/ou des intégrateurs de ce produit ;
   - le ou les systèmes d'exploitation avec lesquels l'application de paiement a été testée ;
   - le logiciel de base de données utilisé ou pris en charge par l'application de paiement ;
   - une brève description de l'application de paiement/la famille de produits (2-3 phrases) ;
   - un schéma de réseau d'une mise en œuvre type de l'application de paiement (pas nécessairement une mise en œuvre spécifique sur le site d'un client) comprenant, à haut niveau :
     - des connexions internes et externes à un réseau de client,
     - des composants au sein du réseau du client, notamment des dispositifs de point de vente, des bases de données et des serveurs Web, le cas échéant,
     - d'autres applications de paiement/composants, le cas échéant.
   - une description ou un schéma de chaque élément de la liaison de communication, notamment dans le cas (1) d'un LAN, WAN ou d'une connexion Internet, (2) d'une communication logicielle hôte à hôte et (3) d'un hôte sur lequel des logiciels sont déployés (par exemple, comment deux processus différents communiquent l'un avec l'autre sur le même hôte) ;
   - un schéma de flux des données illustrant tous les flux de données de titulaire de carte, y compris l'autorisation, la capture, le règlement et rejet de débit, le cas échéant ;

Copyright 2008 PCI Security Standards Council LLC

- une brève description des fichiers et des tables stockant les données de titulaire de carte, étayée par un inventaire créé (ou obtenu auprès du fournisseur de logiciels) et conservé par le PA-QSA dans les documents de travail, cet inventaire devant comprendre pour chaque stockage de données de titulaire de carte (fichier, table, etc.) :
  - la liste de tous les éléments de données de titulaire de carte stockés,
  - la méthode de sécurisation du stockage de données,
  - la méthode de journalisation de l'accès au stockage de données.
- la liste de tous les composants logiciels relatifs à l'application de paiement, y compris les exigences et les dépendances des logiciels tiers ;
- la description des méthodes d'authentification complète de l'application de paiement, notamment le mécanisme d'authentification de l'application, la base de données d'authentification et la sécurité du stockage de données ;
- la description du rôle de l'application de paiement dans une mise en œuvre type et les autres types d'applications de paiement nécessaires pour une mise en œuvre complète du paiement ;
- la description du client type auquel ce produit est vendu (par exemple, PME, groupe, spécifique ou non à un secteur, Internet, artisan) et base de clients du fournisseur (par exemple, segment de marché, grandes entreprises clientes) ;
- la définition de la méthodologie de gestion des versions du fournisseur afin de décrire/d'illustrer la façon dont le fournisseur indique les changements de version majeurs et mineurs à l'aide des numéros de version, et pour déterminer les types de changements que le fournisseur inclut dans ces changements.

Remarque : L'*annexe B : Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS* doit également être renseignée et envoyée avec le rapport complété PA-DSS.

3. Conclusions et observations

- Tous les évaluateurs PA-QSA doivent utiliser le modèle suivant pour présenter des descriptions et conclusions détaillées dans le cadre du rapport.
- Décrivez les tests réalisés autres que ceux inclus dans la colonne Procédures de test.

4. Coordonnées et date du rapport

- Coordonnées du fournisseur de logiciels (notamment l'URL, le numéro de téléphone et l'adresse électronique)
- Coordonnées de l'évaluateur PA-QSA (notamment le nom, l'URL, le numéro de téléphone et l'adresse électronique)
- Coordonnées du principal contact de l'assurance qualité (AQ) du PA-QSA (notamment le nom du contact principal AQ, le numéro de téléphone et l'adresse électronique)
- Date du rapport

Copyright 2008 PCI Security Standards Council LLC

Étapes de mise en conformité avec la norme PA-DSS

Ce document contient le tableau des conditions et procédures d'évaluation de sécurité, ainsi que l'*annexe B : Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS* et l'*annexe C* : *Attestation de conformité*. Le document Conditions et procédures d'évaluation de sécurité détaille les procédures que le PA-QSA doit réaliser. L'*annexe B : Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS* doit être complétée par le PA-QSA pour confirmer l'état et les fonctionnalités du laboratoire de test utilisé afin de mener cette évaluation PA-DSS. L'*annexe C : Attestation de conformité* doit être complétée et signée par le PA-QSA et le fournisseur de logiciels après renseignement du Rapport sur la conformité.

Le PA-QSA doit effectuer les étapes suivantes :

1. Compléter le Rapport sur la conformité en utilisant ce document comme modèle :
    a. Compléter la préface du Rapport sur la conformité, en respectant la section intitulée « Instructions et contenu du Rapport sur la conformité ».
    b. Compléter et documenter toutes les étapes détaillées dans les Conditions et procédures d'évaluation de sécurité, notamment décrire brièvement les contrôles observés dans la colonne « En place » et indiquer tout commentaire. *Remarque : Un rapport contenant des éléments « Pas en place » ne doit pas être transmis au PCI SSC tant que ceux-ci n'ont pas été définis comme « En place ».*
2. Compléter *l'annexe B : Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS.*
3. Compléter et signer l'*Annexe C : Attestation de conformité* (à remplir à la fois par le PA-QSA et par le fournisseur de logiciels).
4. Une fois renseignés, soumettre tous les documents ci-dessus au PCI SSC conformément au *Guide du programme de la norme PA-DSS.*

Guide du programme de la norme PA-DSS

Veuillez vous reporter au *Guide du programme de la norme PA-DSS* pour obtenir des informations sur la gestion du programme PA-DSS, notamment en ce qui concerne les sujets suivants :

- processus de transmission et d'acceptation du rapport PA-DSS ;
- processus de renouvellement annuel pour les applications de paiement comprises dans la liste des applications conformes à la norme PA-DSS ;
- migration des applications conformes au programme PABP vers la liste des applications de paiement conformes à la norme PA-DSS ;
- notification des responsabilités dans le cas où une application de paiement répertoriée serait mise en cause dans un incident de sécurité.

PCI SSC se réserve le droit d'exiger la revalidation en cas de changements importants de la PA-DSS et/ou de vulnérabilités identifiées dans une application de paiement répertoriée.

Copyright 2008 PCI Security Standards Council LLC

Conditions et procédures d'évaluation de sécurité de la norme PA-DSS

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
1. Ne pas conserver la totalité des données de bande magnétique, de code ou de valeur de validation de carte (CAV2, CID, CVC2, CVV2), ou de bloc PIN				
1.1 Ne stocker aucune donnée d'authentification sensible après autorisation (même cryptée) : Les données concernées sont mentionnées dans les exigences suivantes 1.1.1 à 1.1.3. ***Exigence 3.2 des normes PCI DSS*** *Remarque : En interdisant le stockage des données d'authentification sensibles après autorisation, nous partons du principe que la transaction a été soumise au processus d'autorisation et que le client a reçu l'approbation finale de la transaction. Une fois le processus d'autorisation terminé, ces données d'authentification sensibles ne peuvent plus être stockées.*	**1.1** Si les données d'authentification sensibles (voir les exigences 1.1.1 à 1.1.3 ci-dessous) sont stockées avant autorisation, puis supprimées, procurez-vous la méthodologie de suppression des données et vérifiez-la pour déterminer les données irrécupérables. Pour chaque élément de données d'authentification sensibles ci-dessous, réalisez les étapes suivantes après avoir effectué les nombreuses transactions de test simulant toutes les fonctions d'application de paiement afin d'inclure la génération de conditions d'erreur et les entrées de journaux.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
1.1.1 Après autorisation, ne jamais stocker la totalité du contenu d'une quelconque piste de la bande magnétique (au verso d'une carte, sur une puce ou ailleurs). Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique. *Dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique ci-après :* ▪ *le nom du titulaire du compte ;* ▪ *le numéro de compte principal (PAN, Primary Account Number) ;* ▪ *la date d'expiration ;* ▪ *le code de service.* *Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.* *Remarque :* Pour plus d'informations, se reporter au *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*. ***Exigence 3.2.1 des normes PCI DSS***	**1.1.1** Utiliser des méthodes et des outils légaux (outils commerciaux, scripts, etc.)[4] pour examiner toutes les sorties générées par l'application de paiement et vérifier que la totalité du contenu de toute piste de la bande magnétique au verso de la carte n'est pas stockée après autorisation. Inclure les types de fichiers suivants (ainsi que toute autre sortie générée par l'application de paiement) : ▪ données de transaction entrantes ; ▪ tous les journaux (par exemple, transactions, historique, débogage, erreur) ; ▪ fichiers d'historique ; ▪ fichiers trace ; ▪ mémoire non volatile, y compris cache non volatil ; ▪ schémas des bases de données ; ▪ contenu des bases de données.			

[4] Méthode ou outil légal : un outil ou une méthode pour découvrir, analyser et présenter les données légales, fournissant un moyen efficace d'authentifier, de rechercher et de découvrir des preuves informatiques rapidement et précisément. Les méthodes et outils légaux utilisés par les PA-QSA doivent localiser avec précision toute donnée d'authentification sensible écrite par l'application de paiement. Ces outils peuvent être distribués dans le commerce, libres ou développés en interne par les PA-QSA.

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
1.1.2 Après autorisation, ne pas stocker le code, ou valeur de validation de carte (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement), utilisé pour vérifier les transactions carte absente (card-not-present, CNP). *Remarque : Pour plus d'informations*, se reporter au Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS. ***Exigence 3.2.2 des normes PCI DSS***	**1.1.2** Utiliser des outils et/ou des méthodes légaux (outils commerciaux, scripts, etc.)[5] pour examiner toutes les sorties générées par l'application de paiement et vérifier que le code de validation de carte à trois ou quatre chiffres figurant au recto de la carte de paiement ou dans l'espace signature (CVV2, CVC2, CID, CAV2 data) n'est pas stocké après autorisation. Inclure les types de fichiers suivants (ainsi que toute autre sortie générée par l'application de paiement) : ▪ données de transaction entrantes ; ▪ tous les journaux (par exemple, transactions, historique, débogage, erreur) ; ▪ fichiers d'historique ; ▪ fichiers trace ; ▪ mémoire non volatile, y compris cache non volatil ; ▪ schémas des bases de données ; ▪ contenu des bases de données.			
1.1.3 Après autorisation, ne pas stocker de code PIN (Personal Identification Number) ou de bloc PIN crypté. *Remarque : Pour plus d'informations*, se reporter au Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS. ***Exigence 3.2.3 des normes PCI DSS***	**1.1.3** Utiliser des outils et/ou des méthodes légaux (outils commerciaux, scripts, etc.)[5] pour examiner toutes les sorties générées par l'application de paiement et vérifier que les codes PIN et les blocs PIN cryptés ne sont pas stockés après autorisation. Inclure les types de fichiers suivants (ainsi que toute autre sortie générée par l'application de paiement) : ▪ données de transaction entrantes ; ▪ tous les journaux (par exemple, transactions, historique, débogage, erreur) ; ▪ fichiers d'historique ; ▪ fichiers trace ; ▪ mémoire non volatile, y compris cache non volatil ; ▪ schémas des bases de données ; ▪ contenu des bases de données.			

[5] Méthode ou outil légal : un outil ou une méthode pour découvrir, analyser et présenter les données légales, fournissant un moyen efficace d'authentifier, de rechercher et de découvrir des preuves informatiques rapidement et précisément. Les méthodes et outils légaux utilisés par les PA-QSA doivent localiser avec précision toute donnée d'authentification sensible écrite par l'application de paiement. Ces outils peuvent être distribués dans le commerce, libres ou développés en interne par les PA-QSA.

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
1.1.4 Supprimer de façon sécurisée toute donnée de bande magnétique, valeur ou code de validation de carte, et les données de codes ou blocs PIN stockées par les versions précédentes de l'application de paiement, conformément aux normes du secteur relatives à la suppression sécurisée, comme défini, par exemple, par la liste des produits approuvés gérée par le National Security Agency ou par un autre organisme de normalisation ou de réglementation étatique ou national. ***Exigence 3.2 des normes PCI DSS*** *Remarque : Cette exigence s'applique uniquement si les versions précédentes de l'application de paiement stockaient des données d'authentification sensibles.*	**1.1.4.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les revendeurs/intégrateurs : ▪ la suppression obligatoire des données d'historique (données de bande magnétique, codes de validation de carte, codes ou blocs PIN stockés par les versions précédentes de l'application de paiement) ; ▪ la méthode de suppression des données d'historique ; ▪ la mention qu'une telle suppression est nécessaire pour la conformité avec les normes PCI DSS.			
	1.1.4.b Vérifier que le fournisseur propose un outil ou une procédure d'effacement sécurisée pour supprimer les données.			
	1.1.4.c Vérifier, à l'aide d'outils et/ou de méthodes légaux, que l'outil ou la procédure d'effacement sécurisé proposée par le fournisseur supprime les données de façon sécurisée, conformément aux normes du secteur en la matière.			
1.1.5 Supprimer de façon sécurisée toute donnée d'authentification sensible (données de préautorisation) utilisée pour le débogage ou le dépannage et provenant de fichiers journaux, de fichiers de débogage et d'autres sources de données reçues des clients, pour garantir que les données de bande magnétique, les codes ou les valeurs de validation de carte, et les données de codes ou de blocs PIN ne sont pas stockés sur les systèmes des fournisseurs de logiciels. Ces sources de données doivent être collectées en quantités limitées et uniquement lorsque nécessaire pour résoudre un problème, cryptées lors de leur stockage et supprimées immédiatement après utilisation. ***Exigence 3.2 des normes PCI DSS***	**1.1.5.a** Examiner les procédures du fournisseur de logiciels en ce qui concerne le dépannage des clients et vérifier que les procédures comprennent : ▪ la collecte de données d'authentification sensibles uniquement lorsque cela est nécessaire pour résoudre un problème particulier ; ▪ le stockage de telles données à un emplacement spécifique connu dont l'accès est restreint ; ▪ la collecte d'une quantité de données limitée requise pour résoudre un problème particulier ; ▪ le cryptage des données d'authentification sensibles lors de leur stockage ; ▪ la suppression sécurisée des données immédiatement après leur utilisation.			
	1.1.5.b Sélectionner un échantillon de demandes de dépannage récentes émanant des clients et vérifier que chaque événement a respecté la procédure 1.1.5.a.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
	1.1.5.c Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les revendeurs/intégrateurs : ▪ collecter des données d'authentification sensibles uniquement lorsque cela est nécessaire pour résoudre un problème spécifique ; ▪ stocker de telles données uniquement dans des emplacements spécifiques et connus, d'accès restreint ; ▪ collecter les données en se cantonnant à la quantité nécessaire pour résoudre un problème spécifique ; ▪ crypter les données d'authentification sensibles pour leur stockage ; ▪ supprimer ces données immédiatement après leur utilisation, en appliquant un processus sécurisé.			
2. Protéger les données de titulaire de carte stockées				
2.1 Les fournisseurs de logiciels doivent conseiller les clients quant à la suppression des données de titulaire de carte après expiration de la période de conservation définie par le client. ***Exigence 3.1 des normes PCI DSS***	**2.1.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les revendeurs/intégrateurs : ▪ les données de titulaire de carte dépassant la période de conservation définie par le client doivent être supprimées ; ▪ la liste de tous les emplacements où l'application de paiement stocke les données de titulaire de carte (de manière à ce que le client connaisse l'emplacement des données à supprimer).			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
2.2 Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés). *Remarques :* ▪ *Cette exigence ne s'applique pas aux employés et autres parties qui ont un besoin professionnel légitime de voir l'intégralité du PAN.* ▪ *Cette exigence ne se substitue pas aux exigences plus strictes qui sont en place et qui régissent l'affichage des données de titulaire de carte, par exemple, pour les reçus des points de vente (POS).* ***Exigence 3.3 des normes PCI DSS***	**2.2** Examiner l'affichage des données de carte de crédit, y compris mais sans s'y limiter les dispositifs de point de vente, les écrans, les journaux et les reçus, pour vérifier que les numéros de carte sont masqués lors de l'affichage des données de titulaire de carte, à l'exception des personnes ayant un besoin professionnel légitime de consulter les numéros de carte de crédit complets.			
2.3 Rendre le PAN au minimum illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux), en utilisant l'une des approches suivantes : ▪ hachage unilatéral s'appuyant sur une méthode cryptographique robuste ; ▪ troncature ; ▪ Index tokens et Index pads (les pads doivent être stockés de manière sécurisée) ; ▪ cryptographie robuste associée à des processus et des procédures de gestion des clés. En ce qui concerne les coordonnées de compte, au MINIMUM, le PAN doit être rendu illisible. ***Exigence 3.4 des normes PCI DSS*** *Le PAN doit être rendu illisible où qu'il soit stocké, même en dehors de l'application de paiement.* *Remarque : Le terme « cryptographie robuste » est défini dans le* Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.	**2.3.a** Vérifier que le PAN est rendu illisible où qu'il soit stocké, conformément à l'exigence 3.4 des normes PCI DSS.			
	2.3.b Si le fournisseur de logiciel stocke le PAN, qu'elle qu'en soit la raison (par exemple, parce que les fichiers journaux, les fichiers de débogage et d'autres sources de données sont reçues des clients à des fins de débogage ou de dépannage), vérifier que le PAN est rendu illisible conformément à l'exigence 3.4 des normes PCI DSS.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
2.4 Si un cryptage par disque est utilisé (au lieu d'un cryptage de base de données au niveau fichier ou colonne), l'accès logique doit être géré indépendamment des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales). Les clés de décryptage ne doivent pas être liées à des comptes d'utilisateur. ***Exigence 3.4.1 des normes PCI DSS***	**2.4** Si un cryptage par disque est utilisé, vérifier qu'il est mis en œuvre conformément aux exigences 3.4.1.a à 3.4.1.c des normes PCI DSS.			
2.5 L'application de paiement doit protéger les clés cryptographiques utilisées pour le cryptage des données de titulaire de carte contre la divulgation et l'utilisation illicite. ***Exigence 3.5 des normes PCI DSS***	**2.5** Vérifier que l'application de paiement protège les clés contre la divulgation et l'utilisation illicite, conformément aux exigences 3.5.1 et 3.5.2 des normes PCI DSS.			
2.6 L'application de paiement doit mettre en œuvre les processus et les procédures de gestion des clés cryptographiques utilisés pour le cryptage des données de titulaire de carte. ***Exigence 3.6 des normes PCI DSS***	**2.6** Vérifier que l'application de paiement met en œuvre les techniques de gestion des clés conformément aux exigences 3.6.1 à 3.6.8 des normes PCI DSS.			
2.7 Supprimer de façon sécurisée tout élément de clé cryptographique ou cryptogramme stockés par les versions précédentes de l'application de paiement, conformément aux normes du secteur relatives à la suppression sécurisée, comme défini, par exemple, par la liste des produits approuvés gérée par le National Security Agency, ou par un autre organisme de normalisation ou de réglementation étatique ou national. Il s'agit de clés cryptographiques utilisées pour crypter ou vérifier les données de titulaire de carte. ***Exigence 3.6 des normes PCI DSS*** *Remarque : Cette exigence s'applique uniquement si les versions précédentes de l'application de paiement utilisaient des éléments de clé cryptographique ou des cryptogrammes pour crypter les données de titulaire de carte.*	**2.7.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les revendeurs/intégrateurs : ▪ que les éléments cryptographiques doivent être supprimés ; ▪ la méthode de suppression des éléments cryptographiques ; ▪ qu'une telle suppression est nécessaire pour la conformité avec les normes PCI DSS ; ▪ la méthode de recryptage des données d'historique à l'aide de nouvelles clés.			
	2.7.b Vérifier que le fournisseur propose un outil ou une procédure d'effacement sécurisé pour supprimer les éléments cryptographiques.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
	2.7.c Vérifier, à l'aide d'outils et/ou de méthodes légaux, que l'outil ou la procédure d'effacement sécurisé suppriment les données de façon sécurisée, conformément aux normes du secteur en la matière.			
3. Fournir des fonctions d'authentification sécurisées				
3.1 L'installation « prête à l'emploi » de l'application de paiement à l'issue du processus d'installation doit faciliter l'utilisation d'ID d'utilisateur uniques et de l'authentification sécurisée (définies dans les exigences 8.1, 8.2, et 8.5.8 à 8.5.15 des normes PCI DSS) pour tous les accès administratifs et les accès aux données de titulaire de carte. ***Exigence 8.1, 8.2, et 8.5.8 à 8.5.15 des normes PCI DSS***	**3.1.a** Tester l'application de paiement pour vérifier que des ID d'utilisateur uniques et l'authentification sécurisée sont requis pour tous les accès administratifs et les accès aux données de titulaire de carte conformément aux exigences 8.1, 8.2, et 8.5.8 à 8.5.15 des normes PCI DSS.			
	3.1.b Tester l'application de paiement pour vérifier qu'elle n'utilise pas (ou ne requiert pas l'utilisation de) comptes administratifs par défaut pour d'autres logiciels nécessaires (par exemple, l'application de paiement ne doit pas utiliser le compte administratif pour le logiciel de base de données).			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
Remarque : Ces contrôles de mot de passe ne sont pas prévus pour être appliqués aux employés qui n'ont accès qu'à un numéro de carte à la fois pour faciliter une seule transaction. Ces contrôles sont applicables à l'accès par les employés ayant des droits administratifs, à l'accès aux serveurs comprenant des données de titulaire de carte et à l'accès contrôlé par l'application de paiement. *Cette exigence s'applique à l'application de paiement et à tous les outils associés utilisés pour afficher ou accéder aux données de titulaire de carte.*	**3.1.c** Examiner le *Guide de mise en œuvre de la norme PA-DSS* créé par le fournisseur pour vérifier : ▪ qu'il est recommandé aux clients et aux revendeurs/ intégrateurs de ne pas utiliser les comptes administratifs par défaut pour les connexions à l'application de paiement (par exemple, ne pas utiliser le compte « sa » pour l'accès de l'application de paiement à la base de données) ; ▪ qu'il est recommandé aux clients et aux revendeurs/ intégrateurs d'attribuer une authentification sécurisée à ces comptes par défaut (même s'ils ne seront pas utilisés), puis de désactiver ou de ne pas utiliser les comptes ; ▪ qu'il est recommandé aux clients et aux revendeurs/intégrateurs d'associer une authentification sécurisée aux applications et systèmes de paiement chaque fois que possible ; ▪ qu'il est indiqué aux clients et aux revendeurs/intégrateurs comment créer une authentification sécurisée conforme aux normes PCI DSS pour accéder à l'application de paiement, selon les exigences 8.5.8 à 8.5.15 des normes PCI DSS ; ▪ qu'il est indiqué aux clients et aux revendeurs/intégrateurs que la modification des paramètres d'une installation « prête à l'emploi » pour des ID d'utilisateur uniques et l'authentification sécurisée entraîneront le non-respect des normes PCI DSS.			
3.2 L'accès aux PC, serveurs et bases de données hébergeant les applications de paiement doivent requérir un ID d'utilisateur unique et une authentification sécurisée. ***Exigences 8.1 et 8.2 des normes PCI DSS***	**3.2** Examiner le *Guide de mise en œuvre de la norme PA-DSS* créé par le fournisseur pour vérifier qu'il est vivement recommandé aux clients et revendeurs/intégrateurs de contrôler l'accès, à l'aide d'un ID d'utilisateur unique et de l'authentification sécurisée conformes aux normes PCI DSS, à tout PC, serveur et base de données hébergeant des applications de paiement et des données de titulaire de carte.			
3.3 Rendre les mots de passe des applications de paiement illisibles lors de la transmission et du stockage, à l'aide d'une cryptographie performante reposant sur des normes approuvées. *Remarque : Le terme « cryptographie robuste » est défini dans le* Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS. ***Exigence 8.4 des normes PCI DSS***	**3.3** Examiner les fichiers de mot de passe de l'application de paiement pendant le stockage et la transmission pour vérifier que les mots de passe sont toujours illisibles.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
4. Enregistrer l'activité des applications de paiement				
4.1 À l'issue du processus d'installation, l'installation par défaut « prête à l'emploi » de l'application de paiement doit enregistrer tous les accès utilisateur (notamment pour les utilisateurs avec des droits d'administrateur) et permettre de lier toutes les activités aux utilisateurs individuels. ***Exigence 10.1 des normes PCI DSS***	**4.1** Examiner les paramètres d'application de paiement pour vérifier que les pistes de vérification de l'application de paiement sont automatiquement activées ou que les clients peuvent les activer.			
4.2 L'application de paiement doit mettre en œuvre une piste de vérification automatisée pour effectuer le suivi et surveiller l'accès. ***Exigences 10.2 et 10.3 des normes PCI DSS***	**4.2.a** Examiner les paramètres de journalisation de l'application de paiement et vérifier que les journaux contiennent les données requises dans les exigences 10.2.1 à 10.2.7 et 10.3.1 à 10.3.6 des normes PCI DSS.			
	4.2.b Si les paramètres de journalisation de l'application de paiement sont configurables par le client et les revendeurs/intégrateurs, ou si les clients ou les revendeurs/intégrateurs sont responsables de la mise en œuvre de la journalisation, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier que les informations suivantes ont été incluses : ▪ comment définir des paramètres de journalisation conformes aux normes PCI DSS, selon les exigences 10.2.1 à 10.2.7 et 10.3.1 à 10.3.6 des normes PCI DSS ; ▪ mention spécifiant que les journaux ne doivent pas être désactivés, car cela entraînerait la non-conformité avec les normes PCI DSS.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
5. Développer des applications de paiement sécurisées				
5.1 Développer toutes les applications de paiement conformément aux normes PCI DSS (par exemple, authentification et connexion sécurisées) et sur la base des meilleures pratiques du secteur, et incorporer des informations sur la sécurité tout au long du cycle de développement des logiciels. Ces processus doivent inclure ce qui suit : ***Exigence 6.3 des normes PCI DSS***	**5.1** Obtenir et étudier les processus écrits de développement de logiciels afin de vérifier qu'ils sont basés sur des normes sectorielles, que la sécurité est prise en compte tout au long du cycle de vie du produit et que les applications sont développées conformément aux normes PCI DSS. À partir d'un examen des processus écrits de développement de logiciel, des entretiens avec des développeurs de logiciel, ainsi que de l'étude de données pertinentes (documents afférents à la configuration de réseau, données de production et de test, etc.), vérifier ce qui suit :			
5.1.1 Tester tous les correctifs de sécurité, ainsi que toute modification de configuration de système ou de logiciel avant déploiement, y compris mais sans s'y limiter ce qui suit :	**5.1.1** Tous les correctifs de sécurité, ainsi que toutes les modifications de configuration de système ou de logiciel sont testés avant déploiement, y compris mais sans s'y limiter ce qui suit :			
5.1.1.1 Validation de toutes les entrées afin d'empêcher les attaques XSS (Cross-Site Scripting), les attaques par injection, l'exécution de fichier malveillant, etc.	**5.1.1.1** Validation de toutes les entrées afin d'empêcher les attaques XSS (Cross-Site Scripting), les attaques par injection, l'exécution de fichier malveillant, etc.			
5.1.1.2 Validation du traitement approprié des erreurs	**5.1.1.2** Validation du traitement approprié des erreurs			
5.1.1.3 Validation du stockage cryptographique sécurisé	**5.1.1.3** Validation du stockage cryptographique sécurisé			
5.1.1.4 Validation des communications sécurisées	**5.1.1.4** Validation des communications sécurisées			
5.1.1.5 Validation du RBAC (Role-Based Access Control) approprié	**5.1.1.5** Validation du RBAC (Role-Based Access Control) approprié			
5.1.2 Séparation des environnements de développement/test et de production.	**5.1.2** Les environnements de test/développement sont distincts de l'environnement de production, et il existe un contrôle d'accès pour garantir la séparation.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
5.1.3 Séparation des obligations entre les environnements de développement/test et de production.	**5.1.3** Il existe une séparation entre les missions des collaborateurs affectés aux environnements de développement/test et celles des personnels affectés à l'environnement de production.			
5.1.4 Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement.	**5.1.4** Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement, ou sont expurgées avant usage.			
5.1.5 Suppression des données et comptes de tests avant que les systèmes de production ne deviennent actifs.	**5.1.5** Les données de test et les comptes sont supprimés avant que le système de production ne devienne actif.			
5.1.6 Suppression des comptes d'application de paiement personnalisée, ID d'utilisateur et mots de passe avant que les applications ne soient mises à la disposition des clients.	**5.1.6** Les comptes, ID d'utilisateur et mots de passe d'application de paiement personnalisée sont supprimés avant que les applications ne soient mises à la disposition des clients.			
5.1.7 Examen du code de l'application de paiement avant la mise à la disposition des clients après tout changement considérable afin d'identifier toute vulnérabilité de cryptage éventuelle. *Remarque : Cette exigence s'applique à tous les composants d'application de paiement (aussi bien les applications Web internes qu'orientées public), dans le cadre du cycle de développement du système défini par l'exigence 5.1 de la norme PA-DSS et l'exigence 6.3 des normes PCI DSS. Les examens du code peuvent être réalisés par le personnel interne compétent ou par des prestataires tiers.*	**5.1.7.a** Confirmer que le fournisseur examine le code pour toutes les modifications apportées au code personnalisé des *applications internes* (manuellement ou automatiquement), comme suit : ▪ Les modifications de code sont examinées par des individus autres que l'auteur initial du code, qui doivent être compétents en la matière et maîtriser les pratiques de codage sécurisées. ▪ Les corrections appropriées sont implémentées avant la publication. ▪ Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant la publication.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
	5.1.7.b Confirmer que le fournisseur examine le code pour toutes les modifications apportées au code personnalisé des *applications Web* (manuellement ou automatiquement), comme suit : ▪ Les modifications de code sont examinées par des individus autres que l'auteur initial du code, qui doivent être compétents en la matière et maîtriser les pratiques de codage sécurisées. ▪ Les examens du code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé, telles que celles décrites dans le *Guide de l'OWASP (Open Web Application Security Project)* (voir l'exigence 5.2 de la norme PA DSS et l'exigence 6.5 des normes PCI DSS). ▪ Les corrections appropriées sont implémentées avant la publication. ▪ Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant la publication.			
5.2 Développer toutes les applications Internet (internes et externes, y compris l'accès administratif Web au produit) sur la base de principes directeurs en matière de codage sécurisé, tels que ceux de l'OWASP (*Open Web Application Security Project Guide*). Prévenir les vulnérabilités de codage courantes dans les processus de développement de logiciel, afin d'inclure les éléments suivants : *Remarque : Les vulnérabilités décrites aux points 5.2.1 à 5.2.10 de la norme PA-DSS et aux points 6.5.1 à 6.5.10 des normes PCI DSS étaient actualisées dans le guide de l'OWASP au moment de la publication des normes PCI DSS v1.2. Toutefois, si le guide de l'OWASP est mis à jour, il convient d'utiliser la version la plus récente de ces exigences.* ***Exigence 6.5 des normes PCI DSS***	**5.2.a** Obtenir et étudier des processus de développement de logiciel pour toutes les applications basées sur Internet (internes et externes y compris l'accès administratif Web au produit). Vérifier que le processus intègre la formation aux techniques de codage sécurisé pour les développeurs, et que celle-ci est basée sur des directives telles que le Guide de l'OWASP (http://www.owasp.org). Contacter un échantillon de développeurs et obtenir la preuve qu'ils disposent des connaissances nécessaires en techniques de codage sécurisé.			
	5.2.b Pour les applications de paiement incluses dans l'examen, vérifier qu'elles peuvent résister aux vulnérabilités de codage courantes en effectuant un test manuel ou automatique de pénétration utilisant les techniques suivantes :			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
5.2.1 Les attaques par Cross-site scripting (XSS).	**5.2.1** Attaques par Cross-Site Scripting (XSS) (valider tous les paramètres avant l'inclusion).			
5.2.2 Les attaques par injection, notamment les injections de commandes SQL. Considérer également les attaques par injection LDAP et Xpath ainsi que les autres attaques par injection.	**5.2.2** Attaques par injection, par exemple, une injection de commandes SQL (valider l'entrée pour vérifier que les données utilisateur ne peuvent pas modifier le sens des commandes et des requêtes).			
5.2.3 L'exécution de fichiers malveillants.	**5.2.3** Exécution de fichiers malveillants (valider l'entrée pour vérifier que l'application n'accepte pas les noms de fichiers ou les fichiers des utilisateurs).			
5.2.4 Les références d'objets directes non sécurisées.	**5.2.4** Références d'objets directes non sécurisées (ne pas exposer les références d'objets internes aux utilisateurs).			
5.2.5 Les attaques CSRF.	**5.2.5** Attaques Cross-Site Request Forgery (CSRF) (ne pas se fier aux informations d'autorisation ni aux jetons automatiquement envoyés par les navigateurs).			
5.2.6 Les fuites d'information et le traitement inapproprié des erreurs.	**5.2.6** Fuites d'information et le traitement inapproprié des erreurs (ne pas laisser s'échapper d'informations via les messages d'erreurs ou tout autre moyen).			
5.2.7 La rupture dans la gestion des authentifications et des sessions.	**5.2.7** Rupture dans la gestion des authentifications et des sessions (authentifier correctement les utilisateurs et protéger les informations de compte ainsi que les jetons de session).			
5.2.8 Stockage cryptographique non sécurisé.	**5.2.8** Stockage cryptographique non sécurisé (éviter les défauts cryptographiques).			
5.2.9 Les communications non sécurisées	**5.2.9** Communications non sécurisées (crypter correctement toutes les communications authentifiées et sensibles).			
5.2.10 L'impossibilité de limiter l'accès aux URL.	**5.2.10** Impossibilité de limiter l'accès aux URL (appliquer le contrôle des accès de façon cohérente au niveau de la couche présentation et de la logique applicative pour toutes les URL).			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
5.3 Le fournisseur de logiciels doit suivre les procédures de contrôle des changements pour toutes les modifications apportées à la configuration des logiciels. Les procédures doivent inclure ce qui suit : ***Exigence 6.4 des normes PCI DSS***	**5.3.a** Obtenir et examiner les procédures de contrôle des changements du fournisseur pour les modifications logicielles et vérifier que les procédures nécessitent les éléments 5.3.1 à 5.3.4 ci-dessous.			
	5.3.b Examiner les changements récemment apportés aux applications de paiement et remonter à la documentation de contrôle des changements associée. Vérifier que pour chaque changement étudié, ce qui suit a été documenté selon les procédures de contrôle des changements :			
5.3.1 Documentation de l'impact	**5.3.1** Vérifier que la documentation de l'impact sur les clients est comprise dans la documentation de contrôle des changements, et ce pour chaque changement.			
5.3.2 Validation de la gestion par les parties appropriées	**5.3.2** Vérifier que la validation de la gestion par les parties appropriées est présente pour chaque changement.			
5.3.3 Tests de fonctionnalité opérationnelle	**5.3.3** Vérifier que la fonctionnalité opérationnelle a été réalisée pour chaque changement.			
5.3.4 Procédures de suppression et de désinstallation des produits	**5.3.4** Vérifier que des procédures de suppression ou de désinstallation des produits sont préparées pour chaque changement.			
5.4 L'application de paiement ne doit pas être utilisée ni nécessiter de recourir à des services et protocoles inutiles et non sécurisés (par exemple, NetBIOS, partage de fichiers, Telnet, FTP non crypté, etc.). ***Exigence 2.2.2 des normes PCI DSS***	**5.4** Examiner les services système, les démons et les protocoles activés ou requis par l'application de paiement. Vérifier que les services ou les protocoles inutiles et non sécurisés ne sont pas activés par défaut ou requis par l'application de paiement (par exemple, que FTP n'est pas activé ou crypté via SSH ou une autre technologie).			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
6. Protéger les transmissions sans fil				
6.1 Pour les applications de paiement utilisant la technologie sans fil, cette dernière doit être mise en œuvre de manière sécurisée. ***Exigences 1.2.3 et 2.1.1 des normes PCI DSS***	**6.1.a** Pour les applications de paiement développées par le fournisseur à l'aide de la technologie sans fil et d'autres applications sans fil associées à l'application de paiement, vérifier que les applications sans fil n'utilisent pas les paramètres par défaut du fournisseur et sont configurées conformément à l'exigence 2.1.1des normes PCI DSS.			
	6.1.b Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier qu'il indique aux clients et aux revendeurs/intégrateurs que si le sans fil est utilisé, ils doivent installer un pare-feu conformément à l'exigence 1.2.3 des normes PCI DSS.			
6.2 Pour les applications de paiement utilisant la technologie sans fil, l'application de paiement doit permettre de mettre en œuvre les meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste pour l'authentification et la transmission. Les applications de paiement utilisant la technologie sans fil doivent faciliter ce qui suit concernant l'utilisant du WEP : ▪ *Dans le cadre des nouveaux déploiements sans fil, la mise en œuvre du protocole WEP est interdite à compter du 31 mars 2009.* ▪ *Dans le cadre des déploiements actuels, la mise en œuvre du protocole WEP est interdite après le 30 juin 2010.* ***Exigence 4.1.1 des normes PCI DSS***	**6.2.a** Pour les applications de paiement développées par le fournisseur et utilisant la technologie sans fil, ainsi que pour d'autres applications sans fil associées à l'application du fournisseur, vérifier que les meilleures pratiques du secteur (par exemple, IEEE 802.11i) ont été mises en œuvre afin d'appliquer un cryptage robuste pour l'authentification et la transmission conformément à l'exigence PCI DSS 4.1.1.			
	6.2.b Si des clients sont susceptibles de mettre en œuvre l'application de paiement dans un environnement sans fil, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier que les clients et les revendeurs/intégrateurs disposent d'instructions sur les paramètres sans fil conformes aux normes PCI DSS, selon les exigences 1.2.3, 2.1.1 et 4.1.1 de ces normes.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
7. Tester les applications de paiement pour gérer les vulnérabilités				
7.1 Les fournisseurs de logiciels doivent établir un processus afin d'identifier les vulnérabilités en matière de sécurité récemment découvertes (par exemple, s'abonner à des services d'alerte gratuits disponibles sur Internet) et tester leurs applications de paiement par rapport à ces vulnérabilités. Tout logiciel ou système sous-jacent fourni avec ou requis par l'application de paiement (par exemple, des serveurs Web, des bibliothèques tierces et des programmes) doit être inclus dans ce processus. ***Exigence 6.2 des normes PCI DSS***	**7.1.a** Obtenir et examiner les processus pour identifier les nouvelles vulnérabilités et tester les applications de paiement par rapport à ces vulnérabilités. Vérifier que les processus comprennent ce qui suit : ▪ utilisation de sources externes pour les informations sur les vulnérabilités en matière de sécurité ; ▪ tests des applications de paiement par rapport aux nouvelles vulnérabilités.			
	7.1.b Vérifier que les processus d'identification des nouvelles vulnérabilités et de mise en œuvre des corrections dans l'application de paiement sont appliqués à tous les logiciels fournis avec ou requis par l'application de paiement (par exemple, des serveurs Web, des bibliothèques tierces et des programmes).			
7.2 Les fournisseurs de logiciels doivent établir un processus pour le développement et le déploiement à temps des correctifs de sécurité et des mises à niveau, comprenant la mise à disposition de mises à jour et de correctifs de manière sécurisée avec une chaîne de confiance connue et la préservation de l'intégrité du code des mises à jour et correctifs lors de la mise à disposition et du déploiement.	**7.2.a** Obtenir et examiner les processus de développement et de déploiement des correctifs de sécurité et des mises à niveau pour les logiciels. Vérifier que les processus comprennent ce qui suit : ▪ le développement et le déploiement en temps opportun de correctifs pour les clients ; ▪ la mise à disposition sécurisée des correctifs et des mises à jour avec une chaîne de confiance connue ; ▪ la mise à disposition des correctifs et mises à jour d'une façon qui préserve l'intégrité du livrable ; ▪ les tests d'intégrité du correctif ou de la mise à jour par le système cible avant l'installation.			
	7.2.b Pour vérifier que l'intégrité du code des correctifs et des mises à jour est préservée, appliquer le processus de mise à jour avec un code arbitraire et s'assurer que le système ne permettra pas à la mise à jour de s'exécuter.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
8. Permettre la mise en œuvre de réseaux sécurisés				
8.1 L'application de paiement doit pouvoir être mise en œuvre dans un environnement de réseau sécurisé. L'application ne doit pas interférer avec l'utilisation de dispositifs, d'applications ou de configurations requis pour la conformité aux normes PCI DSS (par exemple, l'application de paiement ne peut pas interférer avec une protection antivirus, des configurations de pare-feu ou avec tout autre dispositif, application, configuration requise pour la conformité PCI DSS). ***Exigences 1, 3, 4, 5, et 6.6 des normes PCI DSS***	**8.1** Tester l'application de paiement dans un laboratoire pour obtenir la preuve qu'elle peut être exécutée dans un réseau entièrement conforme aux normes PCI DSS. Vérifier que l'application de paiement n'inhibe pas l'installation de correctifs ou de mises à jour sur d'autres composants de l'environnement.			
9. Les données de titulaire de carte ne doivent jamais être stockées sur un serveur connecté à Internet.				
9.1 L'application de paiement doit être développée de façon à ce que le serveur de base de données et le serveur Web puissent se trouver sur des serveurs différents et que le serveur de base de données ne doive pas obligatoirement se situer dans la DMZ avec le serveur Web. ***Exigence 1.3.2 des normes PCI DSS***	**9.1.a** Pour vérifier que l'application de paiement stocke des données de titulaire de carte sur le réseau interne et jamais dans la DMZ, obtenir la preuve que l'application de paiement n'impose pas de stocker les données dans la DMZ et permettra d'utiliser une DMZ pour séparer Internet des systèmes stockant les données de titulaire de carte (par exemple, l'application de paiement ne doit pas requérir que le serveur de base de données et le serveur Web se trouvent sur le même serveur ou que le serveur de base de données se trouve dans la DMZ avec le serveur Web).			
	9.1.b Si les clients sont susceptibles de stocker les données de titulaire de carte sur un serveur connecté à Internet, examiner le *Guide de mise en œuvre de la norme PA*-DSS préparé par le fournisseur pour vérifier qu'il a été indiqué aux clients et aux revendeurs/intégrateurs de ne pas stocker les données de titulaire de carte sur des systèmes accessibles par Internet (par exemple, le serveur Web et le serveur de base de données ne doivent pas être hébergés sur le même serveur).			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
10. Permettre des mises à jour logicielles à distance sécurisées				
10.1 Si les mises à jour de l'application de paiement sont délivrées via un accès distant sur les systèmes des clients, les fournisseurs de logiciels doivent indiquer à leurs clients d'activer les technologies d'accès à distance uniquement lorsque nécessaire pour effectuer les téléchargements provenant du fournisseur et de les désactiver immédiatement après le téléchargement. Sinon, en cas de livraison via un VPN ou autre connexion haut débit, les fournisseurs de logiciels doivent indiquer aux clients de configurer correctement un pare-feu ou un produit de pare-feu personnel pour sécuriser les connexions permanentes. ***Exigences 1 et 12.3.9 des normes PCI DSS***	**10.1** Si le fournisseur livre l'application de paiement et/ou les mises à jour via un accès distant sur les réseaux du client, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier qu'il contient : ▪ des instructions pour les clients et les revendeurs/intégrateurs en ce qui concerne l'utilisation de technologies d'accès à distance sécurisées conformément à l'exigence 12.3.9 des normes PCI DSS ; ▪ la recommandation pour les clients et revendeurs/intégrateurs d'utiliser un pare-feu ou un produit de pare-feu personnel si l'ordinateur est connecté via un VPN ou une autre connexion haut débit, afin de sécuriser les connexions permanentes conformément à l'exigence 1 des normes PCI DSS.			
11. Permettre un accès à distance sécurisé à l'application de paiement				
11.1 L'application de paiement ne doit pas interférer avec l'utilisation d'un mécanisme d'authentification à deux facteurs. L'application de paiement doit accepter des technologies telles que RADIUS ou TACACS avec jetons, ou VPN avec des certificats individuels. ***Exigence 8.3 des normes PCI DSS***	**11.1** Tester l'application de paiement dans un laboratoire pour obtenir la preuve qu'elle peut être exécutée avec un mécanisme d'authentification à deux facteurs (l'application de paiement ne doit pas empêcher une organisation de mettre en œuvre une authentification à deux facteurs).			
11.2 Si l'application de paiement est accessible à distance, l'accès distant à l'application de paiement doit être authentifié à l'aide d'un mécanisme d'authentification à deux facteurs. ***Exigence 8.3 des normes PCI DSS***	**11.2** Si l'application de paiement est accessible à distance, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur de logiciels et vérifier qu'il contient des instructions pour les clients et les revendeurs/intégrateurs concernant l'utilisation requise d'une authentification à deux facteurs (ID d'utilisateur et mot de passe et élément d'authentification supplémentaire, tel qu'une carte à puce, un jeton ou un code PIN).			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
11.3 Si les fournisseurs, revendeurs/intégrateurs, ou les clients peuvent accéder aux applications de paiement des clients à distance, l'accès distant doit être mis en œuvre de façon sécurisée. ***Exigence 8.3 des normes PCI DSS***	**11.3.a** Si le fournisseur de logiciels utilise des produits d'accès distant pour accéder à distance à l'application de paiement des clients, vérifier que le personnel du fournisseur met en œuvre et utilise des fonctions de sécurité d'accès distant. *Remarque :* Voici des exemples de fonctions de sécurité d'accès distant : ▪ *modifier les paramètres par défaut dans le logiciel d'accès distant (par exemple, modifier les mots de passe par défaut et utiliser des mots de passe uniques pour chaque client) ;* ▪ *autoriser les connexions uniquement depuis des adresses IP/MAC connues ;* ▪ *utiliser une authentification forte et des mots de passe complexes pour les connexions conformément aux exigences 8.1, 8.3, et 8.5.8 à 8.5.15 des normes PCI DSS ;* ▪ *activer la transmission de données cryptées conformément à l'exigence 4.1 des normes PCI DSS ;* ▪ *activer le verrouillage des comptes après un nombre donné de tentatives de connexion infructueuses conformément à l'exigence 8.5.13 des normes PCI DSS ;* ▪ *configurer le système de façon à ce qu'un utilisateur distant doive établir une connexion VPN (Virtual Private Network) via un pare-feu pour que l'accès soit autorisé ;* ▪ *activer la fonction de journalisation ;* ▪ *limiter l'accès aux mots de passe des clients au personnel autorisé des revendeurs/intégrateurs ;* ▪ *définir les mots de passe des clients conformément aux exigences 8.1, 8.2, 8.4, et 8.5 des normes PCI DSS.*			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
	11.3.b Si les revendeurs/intégrateurs ou les clients peuvent utiliser des logiciels d'accès distant, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur de logiciels et vérifier que les clients et les revendeurs/intégrateurs ont eu pour instruction d'utiliser et de mettre en œuvre des fonctions de sécurité d'accès distant. *Remarque :* Voici des exemples de fonctions de sécurité d'accès distant : ▪ *modifier les paramètres par défaut dans le logiciel d'accès distant (par exemple, modifier les mots de passe par défaut et utiliser des mots de passe uniques pour chaque client) ;* ▪ *autoriser les connexions uniquement depuis des adresses IP/MAC connues ;* ▪ *utiliser une authentification forte et des mots de passe complexes pour les connexions conformément aux exigences 8.1, 8.3, et 8.5.8 à 8.5.15 des normes PCI DSS ;* ▪ *activer la transmission de données cryptées conformément à l'exigence 4.1 des normes PCI DSS ;* ▪ *activer le verrouillage des comptes après un nombre donné de tentatives de connexion infructueuses conformément à l'exigence 8.5.13 des normes PCI DSS ;* ▪ *configurer le système de façon à ce qu'un utilisateur distant doive établir une connexion VPN (Virtual Private Network) via un pare-feu pour que l'accès soit autorisé ;* ▪ *activer la fonction de journalisation ;* ▪ *limiter l'accès aux mots de passe des clients au personnel autorisé des revendeurs/intégrateurs ;* ▪ *définir les mots de passe des clients conformément aux exigences 8.1, 8.2, 8.4, et 8.5 des normes PCI DSS.*			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
12. Crypter le trafic sensible transitant par les réseaux publics				
12.1 Si l'application de paiement envoie ou permet d'envoyer des données de titulaire de carte via des réseaux publics, l'application de paiement doit prendre en charge l'utilisation d'une cryptographie et de protocoles de sécurité forts, tels que SSL /TLS et IPSEC (Internet Protocol Security) pour protéger les données de titulaire de carte pendant la transmission sur les réseaux publics ouverts. *Voici quelques exemples de réseaux publics ouverts couverts par les normes PCI DSS :* ▪ *Internet* ▪ *Technologies sans fil* ▪ *Communications GSM (Global System for Mobile)* ▪ *GPRS (General Packet Radio Service)* ***Exigence 4.1 des normes PCI DSS***	**12.1.a** Si l'application de paiement envoie (ou facilite l'envoi) de données de titulaire de carte via des réseaux publics, vérifier qu'une technologie de transmission cryptée sécurisée (par exemple, IPSEC, VPN ou SSL/TLS) est mise à disposition, ou que son utilisation est recommandée.			
	12.1.b Si l'application de paiement autorise la transmission de données sur les réseaux publics, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur, puis vérifier que le fournisseur a recommandé aux clients et aux revendeurs/intégrateurs l'usage d'une technologie de transmission cryptée sécurisée (par exemple, IPSEC, VPN ou SSL/TLS).			
12.2 L'application de paiement ne doit jamais envoyer de PAN non cryptés à l'aide de technologies de messagerie pour les utilisateurs finaux (par exemple, les e-mails, la messagerie instantanée, le chat). ***Exigence 4.2 des normes PCI DSS***	**12.2.a** Si l'application autorise et/ou facilite l'envoi de PAN via des technologies de messagerie pour les utilisateurs finaux, vérifier qu'une solution de cryptographie performante est mise à disposition ou que son utilisation est recommandée.			
	12.2.b Si l'application de paiement autorise et/ou facilite l'envoi de PAN via des technologies de messagerie pour les utilisateurs finaux, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur, puis vérifier que le fournisseur a spécifié des directives aux clients et aux revendeurs/intégrateurs, recommandant l'usage d'une solution qui met en œuvre une cryptographie performante.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
13. Crypter tous les accès administratifs non-console				
13.1 Indiquer aux clients de crypter tous les accès administratifs non-console à l'aide de technologies telles que SSH, VPN ou SSL/TLS pour la gestion par Internet et les autres accès administratifs non-console. ***Exigence 2.3 des normes PCI DSS*** *Ne jamais utiliser Telnet ou rlogin pour les accès administratifs.*	**13.1** Si l'application de paiement ou le serveur autorise l'administration non-console, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur, puis vérifier que le fournisseur recommande d'utiliser SSH, VPN ou SSL/TLS pour le cryptage des accès administratifs non-console.			
14. Gérer la documentation fournissant des instructions et les programmes de formation pour les clients, les revendeurs et les intégrateurs				
14.1 Développer, gérer et diffuser le(s) *Guide(s) de mise en œuvre de la norme PA-DSS* pour les clients, les revendeurs et les intégrateurs. Ce guide doit :	**14.1** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et les processus associés, et s'assurer qu'il est diffusé à tous les utilisateurs appropriés de l'application de paiement (notamment les clients, les revendeurs et les intégrateurs).			
14.1.1 Traiter toutes les exigences du présent document chaque fois que le *Guide de mise en œuvre de la norme PA-DSS* est mentionné.	**14.1.1** Vérifier que le *Guide de mise en œuvre de la norme PA-DSS* couvre toutes les exigences liées présentes dans ce document.			
14.1.2 Inclure une révision au minimum annuelle et des mises à jour afin que la documentation soit actualisée avec tous les changements logiciels majeurs et mineurs ainsi qu'avec les changements apportés aux exigences dans le présent document.	**14.1.2.a** Vérifier que le *Guide de mise en œuvre de la norme PA-DSS* est révisé tous les ans et mis à jour si nécessaire, afin de documenter tous les changements mineurs ou majeurs apportés à l'application de paiement.			
	14.1.2.b Vérifier que le *Guide de mise en œuvre de la norme PA-DSS* est révisé tous les ans et mis à jour si nécessaire, afin de documenter tous les changements apportés aux exigences PA-DSS.			

Copyright 2008 PCI Security Standards Council LLC

Exigences de la norme PA-DSS	Procédures de test	En place	Pas en place	Date cible/ Commentaires
14.2 Développer et mettre en œuvre des programmes de formation et de communication pour s'assurer que les revendeurs et les intégrateurs savent mettre en œuvre l'application de paiement ainsi que les systèmes et les réseaux associés conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux normes PCI DSS.	**14.2** Examiner les supports de formation et le programme de communication pour les revendeurs et les intégrateurs, et confirmer que les supports couvrent tous les éléments indiqués pour le *Guide de mise en œuvre de la norme PA-DSS* tout au long du présent document.			
14.2.1 Mettre à jour les supports de formation annuellement et chaque fois que de nouvelles versions de l'application de paiement sont éditées.	**14.2.1.a** Examiner les supports de formation destinés aux revendeurs et intégrateurs et vérifier qu'ils sont révisés annuellement et lorsque de nouvelles versions de l'application de paiement sont éditées, et mis à jour comme requis.			
	14.2.1.b Examiner le processus de distribution des nouvelles versions de l'application de paiement et vérifier que la documentation mise à jour est bien diffusée avec l'application de paiement mise à jour.			
	14.2.1.c Sélectionner un échantillon de revendeurs et d'intégrateurs et les contacter pour vérifier qu'ils ont bien reçu les supports de formation.			

Copyright 2008 PCI Security Standards Council LLC

Annexe A : Résumé du contenu du *Guide de mise en œuvre de la norme PA-DSS*

Cette annexe a pour but de résumer les exigences PA-DSS correspondant à des sections du *Guide de mise en œuvre de la norme PA-DSS*, afin d'en présenter le contenu et d'expliquer clairement les responsabilités quant à la mise en œuvre des contrôles afférents.

Exigence PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
1.1.4	Supprimer les données d'authentification sensibles stockées par les versions précédentes des applications de données.	▪ Suppression obligatoire des données d'historique (données de bande magnétique, codes de validation de carte, codes ou blocs PIN stockés par les versions précédentes de l'application de paiement). ▪ Méthode de suppression des données d'historique. ▪ Suppression nécessaire pour la conformité avec les normes PCI DSS.	**Fournisseur de logiciels :** Fournir l'outil ou la procédure aux clients pour supprimer les données stockées par les versions précédentes en toute sécurité conformément à l'exigence 1.1.4 de la norme PA-DSS. **Clients et revendeurs/intégrateurs :** Supprimer toute donnée d'historique conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 1.1.4 de la norme PA-DSS.
1.1.5	Supprimer toute donnée d'authentification sensible (préautorisation) recueillie à l'issue du dépannage de l'application de paiement.	▪ Les données d'authentification sensibles (préautorisation) doivent être uniquement recueillies pour résoudre un problème spécifique. ▪ De telles données doivent être enregistrées uniquement à des emplacements spécifiques et connus à accès restreint. ▪ Collecter les données en se limitant à la quantité nécessaire pour résoudre un problème spécifique. ▪ Les données d'authentification sensibles doivent être cryptées pendant lors stockage. ▪ De telles données doivent être supprimées de façon sécurisée immédiatement après leur utilisation.	**Fournisseur de logiciels :** Résoudre les problèmes du client conformément à l'exigence 1.1.6.a de la norme PA-DSS. **Clients et revendeurs/intégrateurs :** Résoudre les problèmes conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 1.1.6.a de la norme PA-DSS.
2.1	Purger les données de titulaire de carte à l'issue de la période de conservation définie par le client.	▪ Les données de titulaire de carte dépassant la période de conservation définie par le client doivent être purgées. ▪ Tous les emplacements où l'application de paiement stocke des données de titulaire de carte sont concernés.	**Fournisseur de logiciels :** Informer les clients que les données de titulaire de carte dépassant les périodes de conservation définies par le client doivent être purgées des emplacements de stockage. **Clients et revendeurs/intégrateurs :** Purger les données de titulaire de carte à l'issue de la période de conservation définie par le client.

Copyright 2008 PCI Security Standards Council LLC

Exigence PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
2.7	Supprimer tout élément de clé cryptographique ou cryptogramme stocké par les versions précédentes de l'application de paiement.	▪ Les éléments cryptographiques doivent être supprimés. ▪ Méthode de suppression des éléments cryptographiques. ▪ Suppression nécessaire pour la conformité avec les normes PCI DSS. ▪ Méthode de recryptage des données d'historique à l'aide de nouvelles clés.	**Fournisseur de logiciels :** Fournir un outil ou une procédure de suppression sécurisée des éléments de clé cryptographiques ou des cryptogrammes stockés par les versions précédentes, conformément à l'exigence 1.1.5 de la norme, et fournir un outil ou une procédure pour crypter de nouveau les données d'historique avec de nouvelles clés. **Clients et revendeurs/intégrateurs :** Supprimer tout élément cryptographique d'historique conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 1.1.5 de la norme PA-DSS.
3.1	Utiliser des ID d'utilisateur uniques et sécuriser l'authentification pour l'accès administratif et l'accès aux données de titulaire de carte	▪ Ne pas utiliser de comptes administratifs par défaut pour les connexions de l'application en ligne. ▪ Associer l'authentification sécurisée aux comptes par défaut (même s'ils ne sont pas utilisés) et désactiver ou ne pas utiliser les comptes. ▪ Utiliser l'authentification sécurisée pour l'application et le système de paiement chaque fois que possible. ▪ Méthode de création d'une authentification sécurisée pour accéder à l'application de paiement conformément aux exigences 8.5.8 à 8.5.15 des normes PCI DSS.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge l'utilisation par le client d'ID d'utilisateur uniques et de l'authentification sécurisée pour les comptes/mots de passe d'application de paiement, conformément aux exigences 8.1 et 8.2 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Mettre en place et gérer des ID d'utilisateur uniques et l'authentification sécurisée, conformément au *Guide de mise en œuvre de la norme PA-DSS et aux exigences* 8.1 et 8.2 des normes PCI DSS.

Copyright 2008 PCI Security Standards Council LLC

Exigence PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
3.2	Utiliser des ID d'utilisateur et sécuriser l'authentification pour l'accès aux PC, serveurs et bases de données	Utiliser des noms d'utilisateur uniques et une authentification sécurisée pour accéder aux PC, serveurs et bases de données comprenant des applications de paiement et/ou des données de titulaire de carte, conformément aux exigences 8.5.8 à 8.5.15 des normes PCI DSS.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge l'utilisation par le client d'ID d'utilisateur uniques et d'une authentification sécurisée pour les comptes/mots de passe si de telles méthodes ont été définies par le fournisseur pour accéder aux PC, serveurs et bases de données, conformément aux exigences 8.1, 8.2 et 8.5.8 à 8.5.15 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Mettre en place et gérer des ID d'utilisateur uniques et l'authentification sécurisée, conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux exigences 8.1, 8.2 et 8.5.8 à 8.5.15 des normes PCI DSS.
4.2	Mettre en œuvre des pistes de vérification automatisées.	▪ Définir des paramètres de journaux conformes aux normes PCI DSS, selon l'exigence 10 des normes PCI DSS. ▪ Les journaux doivent être activés ; leur désactivation entraînera la non-conformité avec les normes PCI DSS.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge l'utilisation par le client de journaux conformes à l'exigence 10 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Mettre en place et gérer des journaux conformes aux normes PCI DSS conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 10 des normes PCI DSS.
6.1	Mettre en œuvre la technologie sans fil de façon sécurisée.	Si une technologie sans fil est utilisée dans l'environnement de paiement, installer un pare-feu conformément à l'exigence 1.3.8 des normes PCI DSS.	**Fournisseur de logiciels :** Indiquer aux clients et aux revendeurs/intégrateurs qu'en cas d'utilisation d'une technologie de pare-feu avec l'application de paiement, les paramètres par défaut du fournisseur de la technologie sans fil doivent être modifiés conformément à l'exigence PCI DSS 2.1.1. **Clients et revendeurs/intégrateurs :** Si la technologie sans fil est mise en œuvre dans l'environnement de paiement par les clients ou les revendeurs/intégrateurs, installer un pare-feu conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 2.1.1 des normes PCI DSS.

Copyright 2008 PCI Security Standards Council LLC

Exigence PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
6.2	Sécuriser les transmissions de données de titulaire de carte sur les réseaux sans fil.	Si l'application de paiement est mise en œuvre dans un environnement sans fil, utiliser les paramètres sans fil conformes aux normes PCI DSS, selon l'exigence 4.1.1 des normes PCI DSS.	**Fournisseur de logiciels :** Indiquer aux clients et aux revendeurs/intégrateurs qu'en cas d'utilisation d'une technologie sans fil avec l'application de paiement, des transmissions cryptées sécurisées doivent être mises en œuvre conformément à l'exigence 4.1.1 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Si la technologie sans fil est mise en œuvre dans l'environnement de paiement par les clients ou les revendeurs/intégrateurs, utiliser des transmissions cryptées sécurisées conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 4.1.1 des normes PCI DSS.
9.1	Stocker des données de titulaire de carte uniquement sur les serveurs non connectés à Internet.	Ne pas stocker de données de titulaire de carte sur les systèmes accessibles via Internet (par exemple, le serveur Web et le serveur de base de données ne doivent pas se trouver sur le même serveur).	**Fournisseur de logiciels :** S'assurer que l'application de paiement ne requiert pas de stocker des données dans la DMZ ou sur des systèmes accessibles via Internet, et permettra d'utiliser une DMZ conformément à l'exigence 1.3.4 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Mettre en place et gérer des applications de paiement de façon à ce que les données de titulaire de carte ne soient pas stockées sur des systèmes accessibles via Internet, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 1.3.4 des normes PCI DSS.
10.1	Livrer les mises à jour des applications de paiement à distance de façon sécurisée.	▪ Recevoir des mises à jour des applications de paiement à distance via des modems sécurisés conformément à l'exigence 12.3 des normes PCI DSS. ▪ Si un ordinateur est connecté via un VPN ou une autre connexion haut débit, recevoir les mises à jour des applications de paiement à distance via un pare-feu ou un produit de pare-feu personnel conformément aux exigences 1 ou 1.3.9 des normes PCI DSS.	**Fournisseur de logiciels :** Livrer les mises à jour des applications de paiement à distance de façon sécurisée, conformément aux exigences 1, 1.3.9 et 12.3.9 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Recevoir des mises à jour des applications de paiement à distance du fournisseur de façon sécurisée conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux exigences 1, 1.3.9 et 12.3.9 des normes PCI DSS.

Copyright 2008 PCI Security Standards Council LLC

Exigence PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
11.2	Mettre en œuvre l'authentification à deux facteurs pour l'accès distant à l'application de paiement.	Utiliser l'authentification à deux facteurs (ID d'utilisateur et mot de passe et élément d'authentification supplémentaire, tel qu'un jeton) si l'application de paiement est accessible à distance.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge l'utilisation par le client de l'authentification à deux facteurs conformément à l'exigence 8.3 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Mettre en place et gérer l'authentification à deux facteurs pour accéder à distance à l'application de paiement, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence PCI DSS 8.3 des normes PCI DSS.
11.3	Mettre en œuvre le logiciel d'accès distant de façon sécurisée.	Mettre en œuvre et utiliser les fonctions de sécurité du logiciel d'accès distant si ce logiciel est utilisé pour accéder à distance à l'application ou à l'environnement de paiement.	**Fournisseur de logiciels :** (1) Si le fournisseur utilise des produits d'accès distant pour accéder aux sites des clients, se servir des fonctions de sécurité d'accès distant, telles que celles spécifiées dans l'exigence 11.3.a de la norme PA-DSS. (2) S'assurer que l'application de paiement prend en charge l'utilisation par le client des fonctions de sécurité d'accès distant. **Clients et revendeurs/intégrateurs :** Utiliser les fonctions de sécurité d'accès distant si vous autorisez l'accès à distance aux applications de paiement, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 11.3.b de la norme PA-DSS.
12.1	Sécuriser les transmissions de données de titulaire de carte sur les réseaux publics.	Mettre en place et utiliser SSL pour sécuriser les transmissions de données de titulaire de carte sur les réseaux publics, conformément à l'exigence 4.1 des normes PCI DSS.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge l'utilisation par le client de transmissions sécurisées des données de titulaire de carte sur les réseaux publics, conformément à l'exigence 4 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Mettre en place et gérer les transmissions sécurisées des données de titulaire de carte conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 4 des normes PCI DSS.

Copyright 2008 PCI Security Standards Council LLC

Exigence PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
12.2	Crypter les données de titulaire de carte envoyées via des technologies de messagerie pour les utilisateurs finaux.	Mettre en œuvre et utiliser une solution de cryptage si les PAN peuvent être envoyés grâce aux technologies de messagerie pour utilisateurs finaux.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge le cryptage par le client des PAN s'ils sont envoyés à l'aide de technologies de messagerie pour utilisateurs finaux, conformément à l'exigence 4.2 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Crypter tous les PAN envoyés à l'aide de technologies de messagerie pour utilisateurs finaux conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 4.2 des normes PCI DSS.
13.1	Crypter les accès administratifs non-console.	Mettre en œuvre et utiliser SSH, VPN ou SSL/TLS pour crypter tout accès administratif non-console à l'application de paiement ou aux serveurs dans un environnement de données de titulaire de carte.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge le cryptage par le client de tout accès administratif non-console, conformément à l'exigence 2.3 des normes PCI DSS. **Clients et revendeurs/intégrateurs :** Crypter tous les accès administratifs non-console, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à l'exigence 2.3 des normes PCI DSS.

Copyright 2008 PCI Security Standards Council LLC

Annexe B : Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS

Pour : *Software Vendor Application Name Version Number*

À chaque évaluation PA-DSS réalisée, le PA-QSA doit compléter ce document afin de confirmer l'état et les capacités du laboratoire utilisé pour les tests effectués lors de l'évaluation PA-DSS. Ce document complété doit être transmis avec le document rempli sur les conditions et procédures d'évaluation de sécurité PA-DSS.

Pour chaque procédure de conformité du laboratoire, indiquer (dans la colonne « Réalisé dans le laboratoire du PA-QSA ou « Réalisé dans le laboratoire du fournisseur ») si le laboratoire utilisé pour l'évaluation et le laboratoire soumis à ces procédures de conformité était le laboratoire du PA-QSA ou bien celui du fournisseur de logiciels.

Décrire l'architecture de test et l'environnement du laboratoire mis en place pour cette vérification PA-DSS :

Décrire de quelle manière un usage de l'application en conditions réelles a été simulé dans le laboratoire pour cette vérification PA-DSS :

Exigence pour le laboratoire	Procédure de conformité du laboratoire	Réalisé dans le laboratoire du PA-QSA	Réalisé dans le laboratoire du fournisseur	Commentaires
1. Installer l'application de paiement en respectant les instructions d'installation du fournisseur ou la formation assurée au client.	**1.** Vérifier que le manuel d'installation du fournisseur ou la formation assurée au client a été appliqué pour procéder à l'installation par défaut de l'application de paiement sur toutes les plates-formes listées dans le rapport PA-DSS.			
2. ***Installer et tester toutes les versions de l'application de paiement listées dans le rapport PA-DSS.***	**2.a** Vérifier que toutes les implémentations courantes (dont les versions spécifiques à une région/un pays) de l'application de paiement à tester ont été installées.			
	2.b Vérifier que toutes les versions et plates-formes de l'application de paiement ont été testées.			
	2.c Vérifier que toutes les fonctionnalités critiques de l'application de paiement ont été testées.			

Copyright 2008 PCI Security Standards Council LLC

Exigence pour le laboratoire	Procédure de conformité du laboratoire	Réalisé dans le laboratoire du PA-QSA	Réalisé dans le laboratoire du fournisseur	Commentaires
3. ***Installer et mettre en œuvre tous les périphériques de sécurité requis par les normes PCI DSS.***	**3.** Vérifier que tous les systèmes de sécurité requis par les normes PCI DSS (par exemple, un pare-feu et des logiciels antivirus) ont été mis en œuvre sur les systèmes de test.			
4. ***Installer et/ou configurer tous les paramètres de sécurité requis par les normes PCI DSS.***	**4.** Vérifier que tous les paramètres système, correctifs, etc., conformes aux normes PCI DSS et se rapportant aux systèmes d'exploitation, logiciels système et applications utilisés par l'application de paiement, ont été mis en œuvre sur les systèmes de test.			
5. ***imuler un usage en conditions réelles de l'application de paiement.***	**5.a** Le laboratoire simule un usage en conditions réelles de l'application de paiement, dont tous les systèmes et applications sur lesquels l'application de paiement est mise en œuvre. Ainsi, la mise en œuvre standard d'une application de paiement peut inclure un environnement client/serveur avec dispositif de point de vente dans la partie accueil de la boutique et un système de back office ou un réseau d'entreprise. Le laboratoire simule la mise en œuvre globale.			
	5.b Le laboratoire utilise uniquement des numéros de cartes de test pour la simulation/les tests, sans avoir recours à de vrais PAN. *Remarque : les cartes de test peuvent généralement être obtenues auprès du fournisseur, ou bien d'un processeur ou d'un acquéreur.*			
	5.c Le laboratoire exécute les fonctions d'autorisation et/ou de règlement de l'application de paiement, et toutes les sorties sont examinées selon l'exigence 6 ci-après.			

Copyright 2008 PCI Security Standards Council LLC

Exigence pour le laboratoire	Procédure de conformité du laboratoire	Réalisé dans le laboratoire du PA-QSA	Réalisé dans le laboratoire du fournisseur	Commentaires
	5.d Le laboratoire et/ou les processus appliquent toutes les sorties générées par l'application de paiement à tous les scénarios possibles, qu'il s'agisse de sorties temporaires, permanentes, de traitement d'erreurs, de mode débogage, de fichiers journaux, etc.			
6. ***Fournir les fonctionnalités nécessaires pour les méthodologies suivantes de test de pénétration et réaliser les tests via celles-ci :***	**5.e** Le laboratoire et/ou les processus simulent et valident toutes les fonctions de l'application de paiement, afin d'inclure la génération de toutes les conditions d'erreur et de toutes les entrées de journaux en utilisant à la fois des données « réelles » simulées et des données non valides.			
	6.a Utilisation de méthodes/d'outils légaux[6] : des méthodes/outils légaux ont été utilisés pour analyser toutes les sorties identifiées, afin d'y rechercher la présence de données d'authentification sensibles (outils commerciaux, scripts, etc.), conformément aux exigences 1.1.1 à 1.1.3 de la norme PA-DSS.[6]			
	6.b Tentative d'exploitation des vulnérabilités OWASP : les vulnérabilités OWASP ont été utilisées pour tenter de lancer un « exploit » de l'application de paiement, conformément aux exigences 5.1.1 à 5.1.10 de la norme PA-DSS.			
7. ***N'utiliser le laboratoire du fournisseur QU'APRÈS avoir vérifié que toutes les exigences sont satisfaites.***	**6.c** Le laboratoire et/ou les processus ont tenté d'exécuter un code arbitraire lors du processus de mise à jour de l'application de paiement : exécution du processus de mise à jour avec un code arbitraire, conformément à l'exigence 7.2.b de la norme PA-DSS.			

[6] Méthode ou outil légal : un outil ou une méthode pour découvrir, analyser et présenter les données légales, fournissant un moyen efficace d'authentifier, de rechercher et de découvrir des preuves informatiques rapidement et précisément. Les méthodes et outils légaux utilisés par les PA-QSA doivent localiser avec précision toute donnée d'authentification sensible écrite par l'application de paiement. Ces outils peuvent être distribués dans le commerce, libres ou développés en interne par les PA-QSA.

Copyright 2008 PCI Security Standards Council LLC

Exigence pour le laboratoire	Procédure de conformité du laboratoire	Réalisé dans le laboratoire du PA-QSA	Réalisé dans le laboratoire du fournisseur	Commentaires
	7.a Si l'utilisation du laboratoire du fournisseur de logiciels est nécessaire (par exemple, si le PA-QSA ne dispose pas du système mainframe, AS400 ou Tandem sur lequel s'exécute l'application de paiement), le PA-QSA peut soit (1) utiliser les équipements prêtés par le fournisseur, soit (2) utiliser les installations de laboratoire du fournisseur, à condition que ceci soit détaillé dans le rapport, accompagné du lieu de déroulement des tests. Dans un cas comme dans l'autre, le PA-QSA a vérifié que les équipements et le laboratoire du fournisseur répondent aux exigences suivantes :			
	7.b Le PA-QSA vérifie que le laboratoire du fournisseur répond à toutes les exigences spécifiées ci-dessus et documente ceci en détail dans le rapport.			
	7.c Tous les tests sont réalisés par le PA-QSA (le fournisseur ne peut pas faire de tests de sa propre application).			
	7.d Tous les tests sont soit (1) réalisés sur site dans les locaux du fournisseur, soit (2) réalisés à distance via une connexion réseau utilisant une liaison sécurisée (par exemple, un VPN).			

Copyright 2008 PCI Security Standards Council LLC

Exigence pour le laboratoire	Procédure de conformité du laboratoire	Réalisé dans le laboratoire du PA-QSA	Réalisé dans le laboratoire du fournisseur	Commentaires
8. ***Appliquer un processus efficace d'assurance qualité (AQ).***	**7.e** Seuls des numéros de cartes de test sont utilisés pour la simulation/les tests, sans avoir recours à de vrais PAN. Ces cartes de test peuvent généralement être obtenues auprès du fournisseur, ou bien d'un processeur ou d'un acquéreur.			
	8.a Le personnel AQ du PA-QSA vérifie que toutes les plates-formes identifiées dans le rapport PA-DSS ont été incluses dans les tests.			
	8.b Le personnel AQ du PA-QSA vérifie que toutes les exigences de la norme PA-DSS ont été testées.			
	8.c Le personnel AQ du PA-QSA vérifie que les configurations et les processus du laboratoire du PA-QSA répondent aux exigences et ont été précisément documentés dans le rapport.			
	8.d Le personnel AQ du PA-QSA vérifie que le rapport rend compte précisément des résultats des tests.			

Copyright 2008 PCI Security Standards Council LLC

Annexe C : Attestation de conformité

Instructions de transmission

L'évaluateur de sécurité qualifié des applications de paiement (PA-QSA) doit remplir ce document qui fait office de déclaration sur l'état de conformité de l'application de paiement vis-à-vis des normes en matière de sécurité des données des applications de paiement (PA-DSS). Remplir toutes les sections applicables de cette attestation de conformité. Transmettre le Rapport sur la conformité avec la norme PA-DSS, cette attestation et l'Annexe B complétée au PCI SSC. Une fois acceptée par le PCI SSC, l'application de paiement sera publiée sur le site Web du PCI SSC comme une application de paiement conforme à la norme PA-DSS.

Le PA-QSA et le fournisseur de l'application de paiement doivent remplir toutes les sections et transmettre ce document au PCI SSC, accompagné de copies de tous les documents de conformité requis, en respectant les instructions du PCI SSC en matière de cryptage et de transmission de rapport.

Partie 1. Informations sur la société PA-QSA

Nom de l'entreprise :					
Nom du principal contact PA-QSA :		*Poste occupé :*			
Téléphone :		*Adresse électronique :*			
Adresse professionnelle :		*Ville :*			
État/province :		*Pays :*		*Code postal :*	
URL :					

Partie 2. Informations sur le fournisseur de l'application de paiement

Nom de l'entreprise :					
Nom du contact :		*Poste occupé :*			
Téléphone :		*Adresse électronique :*			
Adresse professionnelle :		*Ville :*			
État/province :		*Pays :*		*Code postal :*	
URL :					

Copyright 2008 PCI Security Standards Council LLC

Partie 2a. Informations sur l'application de paiement

Lister le ou les noms et numéros de version des applications de paiement incluses dans la vérification PA-DSS :

Fonctionnalités de l'application de paiement (cocher toutes les cases adéquates) :

☐ Point de vente	☐ Panier d'achat	☐ Carte absente
☐ Middleware (intergiciel)	☐ Règlement	☐ Passerelle
☐ Pompe à essence automatisée	☐ Autres (préciser) :	

Marché visé par l'application :

Part 3. Conformité PCI PA-DSS

Partie 3a. Confirmation de l'état de conformité

En se basant sur les résultats mentionnés dans le Rapport sur la conformité avec la norme PA-DSS en date du *(date of ROC)*, *(QSA Name)* certifie l'état de conformité suivant au *(date)* pour la ou les applications et versions identifiées dans la Partie 2a de ce document (cocher une seule case) :

☐	**Pleinement conforme :** Toutes les exigences du Rapport sur la conformité sont notées « En place ». Par conséquent, *(Payment Application Name(s) and Version(s))* est/sont pleinement conforme(s) à la norme PA-DSS.
☐	Le Rapport sur la conformité a été renseigné selon la norme PA-DSS, version *(insert version number)*, conformément aux instructions.
☐	Toutes les informations présentes dans le rapport susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats des évaluations, à tous points de vue.
☐	Aucune preuve de stockage de données de bande magnétique (c'est-à-dire de pistes)[7], de données CAV2, CVC2, CID ou CVV2[8] ou de données PIN[9] suite à l'autorisation d'une transaction sur TOUT fichier ou fonctionnalité généré(e) par l'application n'a été décelée lors de cette évaluation.

Partie 3b. Confirmation de revalidation annuelle :

	Le contenu du Rapport sur la conformité mentionné ci-dessus reste applicable à la version logicielle suivante : *(Payment Application Name and version)*.

Remarque : Remarque : La section 3b se rapporte à l'attestation annuelle requise pour les applications de paiement répertoriées et doit être complétée UNIQUEMENT si aucune modification n'a été apportée à l'application de paiement couverte par le Rapport de conformité susmentionné.

[7] Données de bande magnétique (piste) : Données encodées sur la bande magnétique utilisée pour une autorisation lors d'une transaction carte présente. Les entités ne peuvent pas conserver l'ensemble des données sur bande magnétique après autorisation. Les seuls éléments de données de piste pouvant être conservés sont le numéro de compte, la date d'expiration et le nom du détenteur.

[8] La valeur à trois ou quatre chiffres imprimée sur l'espace dédié à la signature ou sur la face avant d'une carte de paiement, utilisée pour vérifier les transactions carte absente.

[9] Les données PIN (Personal Identification Number, numéro d'identification personnel) désignent le code saisi par le titulaire de la carte lors d'une transaction carte présente, et/ou le bloc PIN crypté présent dans le message de la transaction.

Copyright 2008 PCI Security Standards Council LLC

Partie 3c. Ratification par le PA-QSA et le fournisseur de l'application

Signature du PA-QSA principal ↑	*Date* ↑
Nom du PA-QSA principal ↑	*Poste occupé* ↑
Signature du cadre supérieur du fournisseur de l'application ↑	*Date* ↑
Nom du cadre supérieur du fournisseur de l'application ↑	*Poste occupé* ↑
Nom de l'entreprise fournissant l'application de paiement représentée ↑	

Copyright 2008 PCI Security Standards Council LLC